

North Carolina Department of Information Technology

Enterprise Electronic Forms and Digital Signature

ITS-400335

July 24, 2018

Electronic Copy



*CDW Government LLC
230 N. Milwaukee Ave.
Vernon Hills, IL 60061*




STATE OF NORTH CAROLINA Department of Information Technology	REQUEST FOR PROPOSAL NO. ITS-400335	
	Offers will be publicly opened: July 12, 2018	
	Issue Date: June 11, 2018	
Refer ALL inquiries regarding this RFP to: Kristen Burnette kristen.burnette@nc.gov 919-754-6678	Commodity Number: 208	
	Description: Enterprise Electronic Forms and Digital Signature Capability	
	Using Agency: Multiple State Agencies	
See page 2 for mailing instructions.	Requisition No.: NA	

OFFER AND ACCEPTANCE: The State seeks offers for the Online Services and/or goods described in this solicitation. All offers and responses received shall be treated as offers to contract. The State's acceptance of any offer must be demonstrated by execution of the acceptance found below, and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's offer.

EXECUTION: In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein. By executing this offer, I certify that this offer is submitted competitively and without collusion.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR: CDW Government LLC		
STREET ADDRESS: 230 N. Milwaukee Ave.	P.O. BOX:	ZIP:
CITY, STATE & ZIP: Vernon Hills, IL 60061	TELEPHONE NUMBER: 847-371-5800	TOLL FREE TEL. NO 800-808-4239
PRINT NAME & TITLE OF PERSON SIGNING: Larissa Newman	FAX NUMBER: (847) 465-6800	
AUTHORIZED SIGNATURE: 	DATE: 7/24/2018	E-MAIL: larinew@cdw.com

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ___ days.

ACCEPTANCE OF OFFER: If any or all parts of this offer are accepted, an authorized representative of AGENCY shall affix their signature hereto and this document and the documents identified above shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR AGENCY USE ONLY Offer accepted and contract awarded _____, as indicated on attached certification, by _____ (Authorized representative of DEPARTMENT OF INFORMATION TECHNOLOGY).



One CDW Way
230 N. Milwaukee Ave
Vernon Hills, IL 60061
P: 847.371.5800
F: 847.465.6800
Toll-Free: 800.808.4239
www.cdwg.com/PeopleWhoGetIT

Letter of Transmittal

North Carolina Department of Information Technology
3900 Wake Forest Road
Raleigh, NC 27609

July 24, 2018
RE: ITS-400335

Dear Ms. Burnette,

North Carolina Department of Information Technology (NCDIT) requires an enterprise electronic signature and digital forms solution that is responsive, cost effective, and will help address problems on a large scale. CDW Government (CDW•G) has the right relationships, expertise, and resources to deliver the solution NCDIT needs to be successful.

By choosing CDW•G for this opportunity, North Carolina Department of Information Technology will receive:

Best in Class Solution. CDW•G, in partnership with Adobe, are pleased to offer Adobe Sign as the enterprise electronic forms and digital signature solution for agencies in North Carolina. Known as the leader in e-signatures, Adobe Sign is a secure, compliant, and comprehensive solution that will address all possible concerns. Agencies will receive personalized dedication every step of the way, from helpful training tools, to customer support.

Trusted Partner. CDW has been in partnership with Adobe for 16 years and is recognized as a Platinum Partner, being the #1 largest channel partner in the US and the World. Adobe named CDW its 2017 Worldwide Digital Media Partner of the Year, recognizing our success in driving sales of Adobe digital media solutions. CDW•G and Adobe share a strong relationship that will benefit NCDIT through aggressive pricing, expedited awareness of new products, industry leading software licensing experience, and unwavering support.

Proven, Long Term Relationship. CDW•G has been working with the state of North Carolina for over 20 years. Through several contracts across the state, CDW•G has seen a 4.1% growth from 2016-2017, earning \$19.3 million in revenue. More recently, CDW•G was thrilled to gain partnership with NCDIT in 2016, generating \$73,000 in revenue.

CDW•G looks forward to not just meeting, but exceeding NCDIT's expectations. If you have any questions pertaining to this proposal response, please contact proposal specialist Kaitlin Horne at (312) 547-2777 or via email at kaithor@cdw.com.

Sincerely,

Larissa Newman
Capture Manager

Letter of Transmittal, continued

Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized by the organization to contractually obligate the organization;

Larissa Newman, Capture Manager

Phone: (312) 705-4078

Fax: (312) 752-3619

Email: larinew@cdw.com

Sherri McLean, Deputy Program Manager

Phone: (312) 705-9381

Fax: (312) 705-3791

Email: shermcl@cdw.com

Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized to negotiate the Agreement on behalf of the organization;

Julia Talaski, Contract Negotiator

Phone: (312) 547-2959

Fax: (847) 968-0978

Email: juliisa@cdw.com

Identify the names, titles, telephone and fax number, along with an e-mail address of the person to be contacted for clarification;

Kaitlin Horne, Proposal Specialist

Phone: (312) 547-2777

Fax: (847) 968-0978

Email: kaithor@cdw.com

Acknowledge receipt of any and all amendments to this RFP.

CDW•G acknowledges receipt of Addenda 1, 2, and 3. Please refer to Appendix C, Attachment C for acknowledged amendments.

Points of Contact

As requested per page 4 of Original RFP.

POINTS OF CONTACT: Contact by the Offeror with the persons shown below for contractual and technical matters related to this RFP is only permitted if expressly agreed to by the procurement officer named on page 2, or upon award of contract:

Vendor Contractual Point of Contact	Vendor Technical Point of Contact
CDW Government Street: 120 S. Riverside Chicago, IL 60606 Attn: Sherri McLean	CDW Government, LLC Street: 2001 Edmund Halley Dr. Reston, VA 20191 Attn: Frank Lieberman

State Contractual Point of Contact	State Technical Point of Contact
North Carolina Department of Information Technology Statewide IT Procurement 3900 Wake Forest Road Raleigh, NC 27609 Attn: Kristen Burnette, Contract and Vendor Manager kristen.burnette@nc.gov	North Carolina Department of Information Technology 3700 Wake Forest Road Raleigh, NC 27609 Attn: Samila Mohseni, Enterprise Applications, Director samila.mohseni@nc.gov

Vendor Description

As requested per Section IV.3.b

Detailed description of Vendor's firm should include all of the following:

- i. Full name, address, and telephone number of the organization;

CDW Government, LLC
230. N. Milwaukee Ave.
Vernon Hills, IL 60061
(847) 371-5800

- ii. Date established;

CDW was founded in 1984. In 1998, CDW•G was founded to further support government and education customers.

- iii. Background of firm;

CDW is a leading multi-brand technology solutions provider to business, government, education, and healthcare customers in the United States, Canada, the United Kingdom, and other international locations. We have an expansive network of offices near major cities and a large team of field coworkers across the United States. In 2017, CDW achieved \$15.1 billion in revenue. CDW ranks at number 189 on the FORTUNE 500 list and second within the Information Technology Services category. CDW ranks at No. 5 on CRN's 2017 Solution Provider 500 list.

CDW Government, LLC is the wholly-owned subsidiary of CDW LLC. Our customer base is quite diverse, ranging from state and local government, federal, healthcare, k-12 and higher education.

- iv. Ownership (public company, partnership, subsidiary, etc.);

CDW Government, LLC is the wholly-owned subsidiary of CDW LLC. Our customer base is quite diverse, ranging from state and local government, federal, healthcare, k-12 and higher education.

- v. If incorporated, state of incorporation must be included.

CDW Government LLC is a limited liability company organized in the state of Illinois.

- vi. Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's firm has been in business, whichever is less.

**CDW reports on the last day of the year*

12/31/17:

CDW•G = 1387

Entire CDW = 7617

12/31/16:

CDW•G = 1389

Entire CDW = 7470

12/31/15:

CDW•G = 1408

Entire CDW = 7479

Table of Contents

Tab 1: Letter of Transmittal.....	2
Points of Contact	4
Vendor Description.....	6
Tab 2: Response to Technical Specifications	9
TECHNICAL REQUIREMENTS:	11
TECHNICAL SPECIFICATIONS:.....	17
Tab 3: Completed Cost Offer	58
Tab 4: References	63
Case Studies	64
Tab 5: Financial Information	78
Tab 6: Conflict of Interest.....	86
Tab 7: Errata and Exceptions.....	87
Tab 8: Copy of the Vendor's License and Maintenance Agreements	88
Vendor Utilization of Workers Outside U.S	88
Reseller Documentation.....	89
Adobe Enterprise Term License Agreement	90
CDW's Letter of Authorization for Adobe	103
North Carolina Business License	105
Tab 9: Other Supporting Materials Including Technical System Documentation	107
Attachment F- Incident Response Overview	109
Attachment AA- Adobe Sign Migration Services	115
Attachment AB- Adobe Sign for Microsoft Office 365.....	117
Attachment D- Certifications, ISO, FedRAMP	119
Attachment E- Agreement Encryption Methods	124
Attachment G- Transform Business Processes with Electronic and Digital Signatures.....	128
Attachment H- Audit Trail.....	139
Attachment I- Compliance Overview.....	143
Attachment J- Adobe Sign Technical Overview	148
Attachment K- Archiving Agreements Externally	159
Attachment L- Multilanguage Sending and Signing	170
Attachment M- Business Partners, Integration Solutions.....	174
Attachment N- API Documentation	189
Attachment P- Adobe Sign for Microsoft.....	191
Attachment Q- Adobe Sign Voluntary Product Accessibility Template.....	227
Attachment R- Form Field Validations.....	238
Attachment S- Adobe Sign Workflow Designer	243
Attachment T- Agreement Field Types	254
Attachment U-Set Reminders	260

Attachment V- Adobe Support Policies: Service Level Agreements	265
Attachment W- Adobe Onboarding Program, Adobe Professional Services, Extended Service Offering	278
Attachment Z- Solution Brief	286
Tab 10: Training and Other Materials, Samples, or Examples	288
Attachment O- Admin Guide	289
Attachment X- Implementing Adobe Sign	354
Attachment Y-Adobe Sign User Guide	374
Tab 11: Appendix A: ITS-400335 Entire Solicitation.....	400
Attachment A: Department of Information Technology Terms and Conditions	
Attachment B: Enterprise Security & Risk Management Office (ESRMO) Vendor Assessment Guide	
Tab 12: Appendix B: Completed Enterprise Security & Risk Management Office (ESRMO) Vendor Assessment Guide.....	486
Tab 13: Appendix C:	512
Attachment C: Acknowledged Addenda.....	513

Response to Technical Specifications

- 1) ENTERPRISE ARCHITECTURE STANDARDS: The North Carolina Statewide Technical Architecture is located at the following website: (<https://it.nc.gov/services/it-architecture/statewide-architecture-framework>). This provides a series of domain documents describing objectives, principles and best practices for the development, implementation, and integration of business systems. Agencies and Vendors should refer to these Architecture documents when implementing enterprise applications and/or infrastructure.
- 2) ENTERPRISE LICENSING: In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements. The agreements may be viewed at: <http://it.nc.gov/services/license-and-agreements>
 - a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.

N/A

- b) Identify and explain any components that are missing from the State's existing license agreement.

N/A

- c) If the Vendor can provide a more cost effective licensing agreement, please explain in detail the agreement and how it would benefit the State.

A Statewide Enterprise Term License Agreement (ETLA) provides the best pricing and best overall cost effectiveness.

- *ETLA can be found under the section titled "Copy of Vendor's License and Maintenance Agreements"*
- d) Explain the transportability and transferability of the proposed license agreements. Any licenses or warranties purchased on behalf of the State for this project must be transferable at the time the Vendor is paid under contract for said component

N/A

- 3) VIRTUALIZATION: *Reserved*

- 4) NCID: *Reserved*.

- 5) CLOUD SERVICE PROVIDERS (CSPs): For offers featuring a cloud- hosted solution, Vendors shall describe how the proposed solution will support the agency's information system security compliance requirements as described in the Statewide Information Security Manual, specifically relating to, and without limitation, the sections relating to cloud services: <http://it.nc.gov/statewide-resources/policies>. *The e-Forms/e-Signature Program should be classified as NIST Moderate per the Statewide Information Security Manual and will be required to receive and securely manage data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy.* To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions. Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.

As a Cloud offering, Adobe Sign complies with many commercial and government security standards. Unlike other smaller eSignature only vendors, Adobe provides to customers years of cloud security experience across many products. This experience is based on common commercial and government set of controls to ensure customer data is well protected – this is referred to as the Adobe Common Controls Framework. This ensures that Adobe can meet current and future Statewide information requirements.

- *Please see Attachment D in for the current list of certifications, ISO 27001 Certification, and the FedRAMP certification.*
- SOC 2 Type 2 can be provided upon executing an NDA between State of NC and Adobe. Other material also available upon NDA execution.

- 6) BRANDING: All offers that incorporate State design and branding, as specified by the State, shall adhere to the State style guide. The State style guide is located at: <http://digitalstyle.nc.gov>.
- 7) EQUIVALENT ITEMS: Reserved.
- 8) LITERATURE: All offers shall include specifications and technical literature sufficient to allow the State to determine that the proposed solution substantially meets all specifications. This technical literature will be the primary source for evaluation. If a specification is not addressed in the technical literature it must be supported by additional documentation and included with the offer. Offer responses without sufficient technical documentation may be rejected.
- 9) EQUIVALENT GOODS: Reserved.
- 10) DEVIATION FROM SPECIFICATIONS: Any deviation from specifications indicated herein must be clearly identified as an exception and listed on a separate page labeled "Exceptions to Specification." Any deviations shall be explained in detail. The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.
- 11) SCOPE OF WORK:

In 2013, the General Assembly transferred the responsibility of procuring electronic forms and digital signature services from the Office of the State Controller (OSC) to the Department of Information Technology (DIT) and the agency's State CIO. Thereby, per North Carolina State Legislation, the awarded solution must adhere to several technical requirements (Please see Section III, #12.)

The following language is taken directly from the North Carolina statute:

The proposed digital solution shall adhere to the N.C. Uniform Electronic Transactions Act (NCGS 66311), the Federal Electronic Signatures in Global and National Commerce Act (Title 15), NC eCommerce (NCGS 66- 58.12), NC Cash Management Statute (NCGS 147.86-22(b)), and the Electronic Notary Act (Chapter 10B, Article 2) and the N.C. Electronic Notary Standards (18 NCAC 07C) § 66-58.4. Use of electronic signatures

All public agencies may use and accept electronic signatures pursuant to this Article, pursuant to Article 40 of this Chapter (the Uniform Electronic Transactions Act), or pursuant to other law. (1998-127, s. 1; 2003-233, s. 1; 2007-119, s. 1.)

Based on current usage, the State estimates that the solution will eventually accommodate over 95,000 transactions. The State will proceed with a decentralized approach of the program with minimal central

management of the enterprise form and digital signature solution. This approach will allow the State to enter into contracts with vendors and allow agencies to access services as they need them for the most cost-effective price. Therefore, in addition to solving a wide variety of identity, authentication, confidentiality, data integrity, and non-repudiation (digital signatures) challenges, any vendor partnerships must invoice and provision each individual agency separately.

TECHNICAL REQUIREMENTS:

In accordance with the legislative mandate, the awarded solution must conform with the following requirements. Vendors should read the information regarding each requirement and any corresponding reference, and provide detailed answers when prompted. Note: Solutions not adhering to technical requirements will not be considered by the State.

a) PII (Personal Identifiable Information)

N.C. Gen. Stat. §75-61(10) defines personal identifying information (PII), in part, as “[a] person’s first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b),” and “identifying information” is defined by G.S. § 14-113.20(b) to include Social Security Number or employer taxpayer identification numbers, Driver’s License, State Identification Card, or Passport Numbers, Checking Account Numbers, Savings Account Numbers, Credit Card Numbers, Debit Card Numbers, Personal Identification (PIN) Code as defined in G.S. § 14-113.8(6), Electronic identification numbers, electronic mail names or addresses, internet account numbers, or Internet identification names, Digital Signatures, any other numbers or information that can be used to access a person’s financial resources, Biometric Data, Fingerprints, Passwords and Parents’ legal surnames prior to marriage. Proposed solutions must adhere to PII protection laws.

Therefore, please describe how the solution is PII compliant.

With Adobe Sign, State of NC can create consistent and secure documents to efficiently gather information, signatures and help maintain compliance with State of NC’s own policies or third-party regulations. Customizable templates and fragments make it easy to keep State of NC’s signed document collection consistent and up-to-date. State of NC can also keep sensitive information—such as personally identifiable information (PII)—secure with powerful digital rights management tools.

b) HIPAA (Health Insurance Portability and Accountability Act)

The Contractor agrees that, if the Division determines that some or all of the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended (“HIPAA”), or its implementing regulations, it will comply with the HIPAA requirements and will execute such agreements and practices as the Division may require to ensure compliance. HIPAA forms, instructions and other materials can be located on the HIPAA web site: <http://hipaa.dhhs.state.nc.us/index.html>. If applicable, proposed solutions must adhere to HIPAA laws.

In consideration of this requirement, please describe how the proposed solution is HIPAA compliant. Please note that the State requires a business associates agreement (BAA).

Adobe Sign is Health Insurance Portability and Accountability Act (HIPAA) compliant. The HIPAA helps ensure sensitive patient information is protected. Adobe Sign services in Adobe Document Cloud can be used by any customer that meets the definition of a covered entity as outlined by the Department of Health and Human Services (HHS) and signs a business associate agreement with Adobe.

c) PCI (Payment Card Industry)

The Payment Card Industry (PCI) Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

In consideration of this requirement, please describe how the proposed solution is PCI compliant.

Adobe Sign conforms to PCI DSS—Adobe Document Cloud sign services have achieved Payment Card Industry (PCI) DSS 3.0 compliance as a merchant and service provider. Audited and approved by an independent Qualified Security Assessor, their strict technical and operational controls for handling cardholder data have been awarded an Attestation of Compliance (AoC).

d) FERPA (Family Educational Rights & Privacy Act)

The Family Educational Rights & Privacy Act (FERPA) states that student educational records are subject to 20 U.S.C. 1232g, Family Rights and Privacy Act (FERPA). Therefore, the Vendor must ensure that the proposed solution fully complies with FERPA and every employee responsible for carrying out the terms of this contract is aware of the confidentiality requirements of federal law. In addition, every such employee must sign a confidentiality acknowledgement that indicates that he or she understands the legal requirements for confidentiality. The Vendor is responsible for the actions of its employee and must take all precautions necessary to ensure that no violations occur. Finally, access to personally identifiable student education information shall be limited to those employees who must have access to it in order to perform their responsibilities pursuant to this contract.

In compliance with the law, please describe the following:

- (1) Describe the capabilities of tracking and reporting the application access.

For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time.

Additionally, logging services conduct server-side activity logging to diagnose service outages, specific customer problems and reported bugs. The logs store only account IDs to help diagnose specific customer issues and do not contain sensitive customer account information, such as username/password combinations. Only authorized Adobe technical support personnel and key operational and technical engineering resources can access the logs to diagnose specific issues that may arise.

(2) Describe the solution's approach to handling non-public data at rest and non-public data in motion.

Non-public data at rest is stored on self-encrypting drives using AES 256-bit encryption. Data is encrypted in-motion with AES 128 bit GCM symmetric key cryptographic block ciphers.

(3) Describe the solution's approach for encrypting data such that only the intended recipient can decrypt it.

Please reference Attachment E for details pertaining to this response.

(4) Describe the solution's process for handling and notification of a breach of non-public data.

Adobe continuously monitors the threat landscape, shares knowledge with security experts around the world, swiftly resolves incidents when they occur, and feeds information back to their development teams to help ensure the highest levels of security protections across Adobe products and services.

- Monitoring- We use security information and event management (SIEM) solutions to consume and analyze various data sources. The information we gather helps us detect potential threats and make intelligent, informed decisions about appropriate responses to each threat.
- Threat intelligence- We receive threat intelligence information from industry sources and we gather our own. We use a combination of automation and employee reviewers to filter this intelligence and determine the necessary course of action.
- Knowledge sharing- We collaborate with other technology companies as well as industry organizations like FIRST.ORG to share knowledge and security threat information.
- Issue reporting and resolution- When an incident occurs with an Adobe product or service, either as reported to us by third parties or discovered by Adobe, the Adobe incident response team works with Adobe development teams to identify, mitigate, and resolve the issue as quickly as possible.
- Forensics- We maintain a state-of-the-art forensics lab to perform deep investigations into security issues and help ensure the most comprehensive response possible.
- *Please refer to attachment F for more details.*

(5) For authorization, describe the solution's handling of various roles associated with data access.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These permissions allow the users to access secured data based on their assigned role/authorization.

e) Security

The state potentially handles a large amount of non-public data. Proposed solutions must adhere to North Carolina Statewide IT Security Policies and Standards (<https://it.nc.gov/statewide-information-security-policies>), as they may relate to personal and/or confidential data. Therefore, please address the following:

The State also requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Attachment B provides a high-level view of specific security requirements that are requirements to meet compliance. Vendors must fill out the VENDOR ASSESSMENT GUIDE in Attachment B.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates.

- *Completed Vendor Assessment Guide can be found in Appendix B.*

The following items are security and/or solution requirements; therefore, describe how the solution will accommodate the following:

- (1) The solution must alert the user to any changes to a document after a digital signature has been applied.

The final signed PDF document is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

- (2) The digital signature service component must require users to prove their identity before applying an electronic signature to a document.

In order to verify the identity of a signer, Adobe Sign provides several methods to identify a signer.

The first factor of identity verification is the signer receives an email with a unique URL for them to view and sign the document. By receiving the email and the unique URL in the email, that provides the first level of identity verification. For security, some circumstances may require a second factor of identity verification. The signer must pass the second factor of identity verification in order to view and sign the document.

Adobe Sign provides a number of second factor identity verification methods that can be used to verify a person's identity:

- **Signing Password**

A Signing Password option allows the sender to set a specific password. You can then send that password to your signer to allow them to be able to access and sign the document. The

password is not relayed via email. This password would be communicated to the signer using an alternate method or using an agreed upon password.

- **Phone Verification (Voice or SMS)**

Phone authentication is a two-factor form of signer verification where the signer receives a code unique on their phone via voice or text message and then enters the code to be able to view and sign the document.

- **Knowledge-based Authentication (KBA)** This is a high-level authentication used mainly in financial institutions and other scenarios that demand a strong assertion of the signer's authenticity. The signer is asked several customized, nontrivial questions from their past and they must get them correct, or they can't sign the agreement. This option is only available for Enterprise and Global level accounts, and only can apply to signers in the United States. A third-party performs the Knowledge-based authentication (KBA (powered by InstantID Q&A from LexisNexis Risk Solutions). To successfully sign a document when this feature is enabled, the signer has to provide answers to regarding personal information about themselves. That third-party then uses that information to craft the questions and validate correct responses.

- **Web Identity Verification**

The Web-identity authentication requires signers to log in with their Google, LinkedIn, Facebook, or Twitter identities before viewing and signing the document. Once a signer successfully validates their web identity, this event is recorded in the Audit Report for this transaction as well. In addition to the identity verification options, certain jurisdictions, such as the European Union as part of eIDAS, may require the use of advanced (AdES) or qualified (QES) electronic signatures from an accredited certificate authority (CA) and qualified signature creation devices (QSCDs). These may include devices such as card readers, badges, and other devices. Adobe Sign meets all of these requirements.

- *For more information, see Attachment G: Transform Business Processes with Electronic and Digital Signatures.*

(3) The solution must provide digital certificates to establish non-reputation (i.e. cannot deny receipt or signature).

Adobe Sign provides necessary controls in-place to assist with non-repudiation including the identity of the signer, the integrity of the document, and the intent for the person to sign. All of this is tracked within the audit report. A signer's identity is verified based on the unique URL sent to their email address for signature. Additionally, two-factor identity verification can be used such as passwords, KBA, Social identity, Phone/SMS verification to verify the signer signing a document. At each stage in the workflow, Adobe Sign maintains a secure checksum of the document to ensure both document integrity and confidentiality. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents with a digital signature before distributing it to all participants. The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length cryptographically sound hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity (see the following figure) and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed. The intent of the signer to sign is built into the signing ceremony for a person to "click to sign" to verify their intent to sign a document. All of

this is tracked within the audit report. Furthermore, Adobe Sign meets or exceeds the legal requirements for electronic signatures in many countries.

- (4) The solution must provide digital hashes to establish fixity (i.e. guarantees that digital documents have not been altered since completion).

The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length cryptographically sound hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

To generate the keys used to lock and certify the final signed PDF, Adobe Sign uses specific certificates issued by trusted certificate authorities (CAs) and timestamp authorities (TSAs). In certain circumstances, Adobe Sign can be configured to issue certified documents using government-required CAs, such as in Switzerland and India. PKI keys used to certify the final PDF are stored in a hardware security module to prevent online attacks and tampering.

TECHNICAL SPECIFICATIONS:

Means, as used herein, a specification that documents the requirements of a system or system component. It typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance standards, or similar terms. Substantial conformity with technical specifications is required.

- a) **Site and System Preparation:** Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. The Vendor shall advise the State of any site requirements for any Deliverables required by the State's specifications. Any alterations or modification in site preparation which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.
- b) **Specifications:** The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and only processes, configuration, material and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified. See, Acceptance Criteria, below.
- c) **Directions:** Please describe how the proposed solution will meet the following technical specifications, including capabilities, features, and limitations. *Note: Vendors are encouraged to align responses with the technical specifications' outline shown below.*

1) General Features

Provide the general features of the proposed solution. Please include the following information:

- a) Use this prompt to articulate an understanding of the state's need as well as any value-added services relevant to this RFP.

Adobe Sign helps an organization replace paper-and-ink signature processes with 100% digital workflows. With Adobe document cloud Sign solution, you can send, sign, track, and manage signature process and electronically sign digital documents on any device, from any location. Adobe Sign meets or can be configured to meet the compliance requirements for many industry and regulatory standards. As a robust cloud-based service, Adobe Sign securely handles large volumes of e-signature processes.

With Adobe Sign, users can reduce signing and approval processes from days to minutes, improve staff productivity and mobility, and create great customer experiences. Customers choose Adobe Sign because of its remarkably simple user experience, robust capabilities, and superior integrations, which minimize deployment time.

Adobe is a well know company and many Sign customers are already very familiar with many Adobe products such as Acrobat and Creative Cloud. By using Sign as part of their existing toolset or by itself, State of NC agencies can easily adapt Sign into their everyday workflow. Our post-sales enablement of customer support, on-boarding specialists and customer success managers are second to none and are ideal to making sure NC agencies can best utilize their

investment into Adobe Sign. This includes best practices, knowledge transfer, use case utilization, and many other benefits.

- b) Address the solution's capacity to include ad hoc workflow routing rules, based on unique business rules defined for document(s) and signature requirements.

With Adobe Sign, administrators can design and manage ad hoc workflow routing rules easily with an intuitive drag-and-drop editor. It's easy to specify: documents to be included in an agreement; characteristics of the participants, including predefined names and roles; form fields to be pre-filled by the sender; agreement expiration or password options; and more.

- c) Can the solution deliver business process workflow for documents, from originator to signatories?

Yes, Adobe Sign delivers business process workflow for documents, from originator to signatories. It offers workflow customization solutions that span the full range of touchpoints, letting you automate signature processes and speed business across your entire organization. Adobe offers two powerful and easy-to-use options that let administrators or business analysts customize signing workflows for their organization — with no “coding” required.

Workflow Designer lets you create easy-to-follow “send” experiences for your users so process steps can be followed consistently every time. With this tool, administrators can design and manage workflow templates easily with an intuitive drag-and-drop editor. It's easy to specify: documents to be included in an agreement; characteristics of the participants, including predefined names and roles; form fields to be pre-filled by the sender; agreement expiration or password options; and more.

There are also options to use Out of Box integrations with other workflow engines, such as Adobe's own AEM Forms, Nintex and Thinksmart for more advanced and flexible routing of documents, form management and back end-integrations with no or limited coding required. Of course, Adobe Sign APIs can also be used for programmatic control of the workflow or integrations with other Workflow engines.

- d) Can the solution integrate with global address books or pull users into a centralized address book?

Yes. You can use a CSV file to import your recipients' email addresses and merge custom data into fields on the document for each recipient. CSV stands for Comma-Separated Value and Excel files can be saved in this format.

- e) Address whether the solution will permit external party signing, including two-factor or multi-factor authentication. Provide examples.

Yes, Adobe Sign permits external party signing. In order to verify the identity of a signer, Adobe Sign provides several methods to identify a signer. The first factor of identity verification is the signer receives an email with a unique URL for them to view and sign the document. By receiving the email and the unique URL in the email, that provides the first level of identity verification. For security, some circumstances may require a second factor of identity verification. The signer must pass the second factor of identity verification in order to view and sign the document.

Adobe Sign provides a number of second factor identity verification methods that can be used to verify a person's identity:

Signing Password:

A Signing Password option allows the sender to set a specific password. You can then send that password to your signer to allow them to be able to access and sign the document. The password is not relayed via email. This password would be communicated to the signer using an alternate method or using an agreed upon password.

Phone Verification (Voice or SMS):

Phone authentication is a two-factor form of signer verification where the signer receives a code unique on their phone via voice or text message and then enters the code to be able to view and sign the document.

- f) Describe the capability to establish evidentiary requirements for signed documents.

An audit document is created for each document which enters the Adobe Sign system and is resident on the server indefinitely as an encrypted, VeriSign certified PDF file.

As the signing process progresses, events are added to the document.

Upon successful signing of the document a link to a web-accessible audit document is stored as a hyperlink attached to each signature panel on the document.

Note: This audit document will remain available for the purposes of evidentiary or non-repudiation indefinitely on the Adobe Sign Service, even after any potential future termination of your licensing of the service. Adobe is providing not only a document processing, routing and signing solution, but also key tracking and authentication records that remain a critical component of the evidence of legality of your documents. For that reason, we will continue to provide you access to these audit records indefinitely.

- g) Describe the process of creating new forms and templates.

With Adobe Sign, the users can use existing templates, or upload new documents, modify them to include signature fields and use them as templates for future signature requirements. This document can then be added as a template to the library and used any number of times to collect signatures from multiple users.

- h) Address whether each person in the workflow is given the opportunity to review all documents, with confirmation opportunity, before the transaction continues.

Adobe Sign supports this, for both the sender and the signer of the contracts. For the sender of the document, they can initiate the review workflow to review and confirm the document before being sent out for signature. And for the signer, during the Signing Ceremony, the participant will view the rasterized view of the document pages rendered in a web browser. This would enable the signer to review the document before signing.

- i) The State needs the signing process to be simple, and require very few steps for users. The steps required to secure signatures should not become more burdensome for any staff involved than current paper processes. Therefore, describe if the solution configures predefined workflow routing rules based on specific business rules defined for document(s) and signature requirements.

Yes. Adobe Sign offers workflow customization solutions that span the full range of touchpoints, letting you automate signature processes and speed business across your entire organization. Adobe offers two powerful and easy-to-use options that let administrators or business analysts customize signing workflows for their organization — with no “coding” required.

Workflow Designer lets you create easy-to-follow “send” experiences for your users so process steps can be followed consistently every time. With this tool, administrators can design and manage workflow templates easily with an intuitive drag-and-drop editor. It's easy to specify: documents to be included in an agreement; characteristics of the participants, including predefined names and roles; form fields to be pre-filled by the sender; agreement expiration or password options; and more.

- j) Describe the solution's capacity to store completed, digitally signed document(s), on the State's own Document Management System; Include whether the:

- (1) Solution supports grouping and/or compartmentalization of originators (i.e. by department, function, division, section) so that documents may not be visible to disparate workgroups.

By default, the final signed documents are stored on the Document Cloud servers indefinitely. However, Adobe also provides turn-key integrations into a number of the State's own document management systems to store completed, digitally signed document(s). For example, Apttus, SAP Ariba, SAP CLM, Selectica (Determine), Determine, Microsoft SharePoint, Box, ASC, IBM Emptoris, Intelligent Contract, McKesson, Oracle, Revitas, SciQuest, SpringCM, Salesforce Steelbrick, Dropbox, and many others.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These roles and permissions allow State of NC to create user groups and/or compartments of originators (i.e. by department, function, division, section) such that specific documents will be visible to only specific work user groups and may not be visible to disparate work user groups.

- (2) Originators monitor the progress and status of transactions they and/or their workgroups have initiated.

Yes, the audit trail can be exported to csv format for every document and can be stored and accessed at later stages. This can be done by navigating to the Manage Tab of the Adobe Sign interface, selecting the agreement for which audit trail is required, and downloading the detailed audit trail from the History tab. Users can also run a report on transactions sent from users in the account. You can also export a CSV file with the raw data generated from the report.

- k) Describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.

Adobe Sign is a 100% browser-based system and can run on any device with browser support. Please visit <https://helpx.adobe.com/sign/system-requirements.html> for a complete listing of the minimum system requirements.

- l) Describe if the solution facilitates digital signing of documents on IOS, Android, and Windows smart phones. Specify minimum software versions supported.

Adobe provides both a Web and Mobile solution. The application can be used to request signatures from others using a browser or mobile device. Your signers just click a link to open

and e-sign from any connected device, be it a mobile phone, tablet, kiosk, signature pad or any other mode of technology which involves a hardware to sign and a web browser (or HTML) support. The mobile/smartphone app of Adobe Sign is available on Android and iOS operating systems.

The following are the minimum software versions supported: iOS 11+ or Android 7+.

- m) Also include whether the solution facilitates digital signing of documents on IOS, Android, and Windows mobile tablet devices. Specify minimum software versions supported.

Adobe provides both a Web and Mobile solution. The application can be used to request signatures from others using a browser or mobile device. Your signers just click a link to open and e-sign from any connected device, be it a mobile phone, tablet, kiosk, signature pad or any other mode of technology which involves a hardware to sign and a web browser (or HTML) support. The mobile/smartphone app of Adobe Sign is available on Android and iOS operating systems.

The following are the minimum software versions supported: iOS 11+ or Android 7+.

- n) Address if the solution can create and manage multiple levels of system access.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These roles and permissions allows State of NC to create and manage multiple levels of system access for different users.

- o) Describe if the solution will provide a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that: (1) the electronic document was not altered without detection during transmission or at any time after receipt; (2) any alterations to the electronic document during transmission or after receipt are fully documented.

Yes. For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time.

- p) Clarify that the solution disallows any form of unauthorized copying or pasting signatures.

Yes. Adobe Sign solution disallows any form of unauthorized copying or pasting signatures.

Adobe Sign only allows for three signature styles, which can be implemented by State of NC as per the requirements:

1. Script-like font: This is the default value and the favored style currently. Adobe Sign applies a font to your name to achieve the appearance of a handwritten signature.
2. Biometric: Draw your signature with a mouse, a stylus, or your finger
3. Signature Image: If you have an actual image of your signature, you can upload that to the system, and Adobe Sign applies that image as your signature when you sign.

- q) Describe if the solution will determine if any modifications were made after the signature for the relevant sections were attached and disallow modifications or invalidate corresponding section that was modified.

The final signed PDF document is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign

seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

- r) Explain if the solution will contain the copy of record, which will include

For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time.

- *Please refer to Attachment H for detailed inputs.*

- (1) All electronic signatures contained in or logically associated with that document.

Please refer the response of Question No. (1.r)

- (2) The date and time of receipt.

Please refer the response of Question No. (1.r)

- (3) Any other information used to record the meaning of the document or the circumstances of its receipt.

Please refer the response of Question No. (1.r)

- (4) Other, such as authorized system ID of signature owner, authorized computer ID, smart device ID such as MAC address, location data, etc.

Please refer the response of Question No. (1.r)

- (5) Detection of unauthorized data modification and place obvious marker on the document – electronic version and paper version.

The final signed PDF document is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

- (6) A function to alert users of needed actions.

Adobe Sign uses email for signature event notifications. Notifications are available for the following events:

- When a document is viewed
- When a document is sent
- When a document is signed or approved
- When a document is declined
- When a document is forwarded
- When a document is uploaded by a sender
- When an agreement is expired
- When an email is bounced
- When a document is not viewed in a specified time
- When a document is not signed or approved in a specified time
- When a document is viewed but not signed in a specified time
- When a document will expire

You can customize your alerts using the Settings area on the portal. You can also have different settings for agreements sent directly to you and accounts that share information with you. The notifications and reminder can be automated as well as modified as per the need.

2) Product Strategy Roadmap

The state needs a fully-developed plan Provide a 12-month Vendor product strategy as it relates to the solution proposed.

We plan to continue to market the benefits of our Document Cloud solutions to individuals as well as small and medium-sized businesses, large enterprises and government institutions around the world and increase our seat penetration in these markets through the utilization of our corporate and volume licensing programs.

We also intend to increase our focus on marketing and licensing solution in targeted vertical markets such as education, financial services, telecommunications and government, as well as on expanding into emerging markets, while simultaneously enhancing and building out the delivery of cloud-based document services to our Acrobat and Adobe Acrobat Reader users.

We intend to continue to promote the capabilities of our cloud-based document solution, such as its integration with users' Dropbox documents, to millions of Acrobat users and hundreds of millions of Adobe Acrobat Reader users. We believe that by growing the awareness of Sign services in the broader contract delivery and signing market and continuing to add new capabilities to this offering, we can help our customers migrate away from paper-based express mailing and adopt our solution, growing our revenue with this business in the process.

3) Disaster Recovery and Hosting Facilities

The state needs to understand the hosting facilities, capabilities and disaster recovery capabilities of the proposed solution, and requires an application disaster recovery plan as well. In addition to these needs, please address the following:

- a) Explain how the vendor will work with the state to develop this plan and integrate it with agency operation.

To support Adobe Document Cloud Sign services, Adobe maintains equipment in geographically dispersed data centers. At any given time, only one data center is "live," while a secondary site acts as a warm disaster recovery site in the event the production site goes offline. All customer data is continuously replicated in real time between the two sites, enabling

a failover should the need arise. The data replicated between the primary data center and the disaster recovery site includes all customer documents, agreements and user information. Data replication is managed over a fully encrypted channel between the data centers. All product and infrastructure changes are kept in sync between the primary data center and the disaster recovery site so that any failover is seamless to Adobe customers.

- b) The data that is stored in this application's database may be confidential and if so, must follow HIPAA, FERPA, PII and PCI compliance. Explain how the vendor will protect this data in the case of an event that requires execution of the disaster recovery plan.

Backed by more than a thousand security features, processes, and controls, Adobe Sign is certified compliant with the industry's most rigorous security standards, including SOC 2 Type 2, ISO 27001, and PCI DSS used in the Payment Card Industry. Adobe Sign complies with industry-specific regulatory requirements, such as HIPAA, FERPA, GLBA, and the Food and Drug Administration (FDA) 21 CFR Part 11 regulation in the United States.

Additionally, Adobe Document Cloud Adobe Sign services managed data center is audited annually to ensure that it meets or exceeds SSAE 16 Type II SOC 2 requirements. The Statement on Standards for Attestation Engagements (SSAE) No. 16 measures the controls relevant to financial reporting, and the Service Organization Controls 2 (SOC 2) measures the IT controls of security and availability

Adobe Sign has also been granted FedRAMP Tailored certification by the US Government.

- *Additional information can be found by referencing Attachment I.*

Data replication between primary data center and the disaster recovery site is managed over a fully encrypted channel. In this way, the confidential data stored in primary data center will be protected in case of an event that requires execution of the disaster recovery plan.

- c) Describe the hosting facilities. Use diagrams where appropriate. Consider the following aspects:

The Adobe Sign service in North America is hosted on Amazon Web Services (AWS) in two separate active/passive data center configurations. Customers are assigned to either the NA1 or NA2 configuration. The NA1 configuration contains three simultaneously active data centers hosted in Virginia that replicate to three passive data centers in Oregon for disaster recovery. The NA2 configuration contains three simultaneously active data centers hosted in Oregon that replicate to three passive data centers in Virginia for disaster recovery. Each individual data center is implemented in a separate Amazon facility and designed to handle Adobe Sign transactions simultaneously, providing for superior performance, scalability, and redundancy. Additional details are available under NDA.

- i) Who is the hosting provider? Where is the primary site? Where is the disaster recovery site?

The Adobe Sign service in North America is hosted on Amazon Web Services (AWS) in two separate active/passive data center configurations. Customers are assigned to either the NA1 or NA2 configuration. The NA1 configuration contains three simultaneously active data centers hosted in Virginia that replicate to three passive data centers in Oregon for disaster recovery. The NA2 configuration contains three simultaneously active data centers hosted in Oregon that replicate to three passive data centers in Virginia for disaster recovery.

- ii) Explain if the hosting facilities are SAS 70 II compliant and/or compliant with SSAE 16 reporting standards, please provide copies of the most recent audit(s).

Yes. The Statement on Standards for Attestation Engagements (SSAE) No. 16 for Service Organization Controls (SOC) are a series of IT controls for security, availability, processing

integrity, and confidentiality (Type 2). SSAE 16 SOC 2 is designed to help organizations comply with the Sarbanes-Oxley Act (SOX). Adobe Sign has a SOC 2 Type 2 (security & availability) attestation.

These audit copies are confidential and can't be shared in this forum. More details are available under NDA and review with our security team.

iii) What is the data center's classification (Tier 1, Tier 2 etc.)?

The Adobe Sign service infrastructure resides in American National Standards Institute (ANSI) tier 4 data centers managed by our trusted cloud service provider, Amazon Web Services (AWS).

iv) What policies are in place to thwart insider breaches?

- Please refer the sections Network protection, Encryption and Compliance in the Adobe Sign Technical Overview document by referencing *Attachment J*

v) What is the process for background checks? Who are they performed by, for which employees, are the checks performed at employment, yearly, etc.

Adobe obtains consumer background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background; work history; court records, including criminal conviction records; and references obtained from professional and personal associates, each as permitted by applicable law. These background check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the U.S., Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local law.

vi) Will all customer data be housed within the continental United States?

Yes. All customer data will be housed within the continental United States (Virginia & Oregon).

vii) Are there any circumstances when the solution would store customer data and intellectual property outside of the United States or with a non-USA owned institute?

No. All customer data will be housed within the continental United States (Virginia & Oregon).

4) Data Management

a) Describe how data is archived and/or purged.

Archives are perfect for keeping backup copies of the agreements you've sent. Adobe Sign supports archival of documents through a single click from the Dashboard itself.

- *For a complete archival process, please reference Attachment K.*

State of NC can also leverage external archival to archive copies of signed agreements to any email address or to Box and Evernote. A copy of the Signed and Filed email is sent to either the email address you provide or to the service you set up.

- *For more details, refer to Attachment K.*

- b) The State must receive an attestation letter explaining how the Vendor destroyed the data when the State separates from the Vendor. Please acknowledge that the solution will supply such communication.

At the end of contract/service, the customer must call Adobe's Customer Support Center in order for Adobe to make the appropriate API calls to extract customer data. This data will then be placed into a file server that the customer has access to.

The format will be either the original uploaded document format, or Certified PDF for signed documents. Audit trail information is retained indefinitely for regulatory compliance.

Adobe can further discuss the legal documentation needed upon termination of any contract and the destruction of customer data.

- c) Describe how the state will get its data back in a form that can be used. What costs will be involved if any?

At the end of contract/service, the customer must call Adobe's Customer Support Center in order for Adobe to make the appropriate API calls to extract customer data. This data will then be placed into a file server that the customer has access to.

The format will be either the original uploaded document format, or Certified PDF for signed documents.

No additional costs are involved.

- d) How is the data destroyed at the end of a term contract?

At the end of contract/service, the customer must call Adobe's Customer Support Center in order for Adobe to make the appropriate API calls to extract customer data. This data will then be placed into a file server that the customer has access to.

The format will be either the original uploaded document format, or Certified PDF for signed documents. Audit trail information is retained indefinitely for regulatory compliance unless directed by a customer via documentation to remove all audit trail information.

- i) Address how workflows, meta-data and configurations will be transferred to the state.

A customer always has access to meta-data for their transactions and can be extracted through exports and reporting. Workflows and configurations such as templates are not customer accessible for downloading but could be transferred into another Adobe Sign account by customer support.

5) Audit

The state retains the right to audit the physical environment (could apply to production, secondary site, etc.) where the vendor application/service is hosted per the vendor proposal. Therefore, describe what processes the solution has in place to allow this audit?

- a) Describe if the solution will provide a retrievable audit trail.

Logging services conduct server-side activity logging to diagnose service outages, specific customer problems and reported bugs. The logs store only account IDs to help diagnose specific customer issues and do not contain sensitive customer account information, such as username/password combinations. Only authorized Adobe technical support personnel and key operational and technical engineering resources can access the logs to diagnose specific issues that may arise.

Additionally, for every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved,

identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded or retrieved at any time.

System logs can be retrieved by support/operations and provided to auditors as needed.

- b) Supply the chain of custody for obtaining the record of copy.

As described above, audit trail documents are obtained directly by the customer from within their own Sign account. Other logs can be obtained from customer support.

- c) Address if the solution can export capabilities for the audit trail data. List possible export formats.

The audit trail can be exported to csv format for every document and can be stored and accessed at later stages. This can be done by navigating to the Manage Tab of the Adobe Sign interface, selecting the agreement for which audit trail is required, and downloading the detailed audit trail from the History tab. Users can also run a report on transactions sent from users in the account. You can also export a CSV file with the raw data generated from the report.

- d) Describe if audit event details are available to customer in a reusable format (i.e. CSV, Excel, PDF).

The audit trail can be exported to csv format for every document and can be stored and accessed at later stages. This can be done by navigating to the Manage Tab of the Adobe Sign interface, selecting the agreement for which audit trail is required, and downloading the detailed audit trail from the History tab. Users can also run a report on transactions sent from users in the account. You can also export a CSV file with the raw data generated from the report.

- e) Describe how the Audit trail is stored and secured against tampering.

Audit reports are certified with a digital certificate to make them tamper-evident PDFs.

- f) The solution must track every event in the signature process. Therefore, describe to what degree such details and events are being stored.

For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time.

- *For more detailed inputs, please refer to Attachment H.*

- g) Explain how consent from users to use the service is tracked as an auditable action.

Yes, you can present users with disclosures and opt out options. When a person chooses the option to refuse to sign, they are prompted to provide a reason back to the sender. Adobe Sign allows you to add a consent clause to your agreements and a term of use for signers to agree to conduct business electronically. When a signer clicks the blue "click to sign" button during the signing ceremony they verify their intent to sign the document and accept the terms of use of the service. Record of this intent to sign the document is tracked in the audit report.

6) NCID

For Identity Management, the state has invested in a common solution called NCID. NCID is the State's enterprise identity management (IDM) service and is operated by the North Carolina Office of Information Technology Services. (The details of NCID can be found at: <https://it.nc.gov/ncid/>.) Additional information regarding this service can be found in the ITS Service Catalog at: <http://www.its.state.nc.us/ServiceCatalog/Index.asp> (see Identity Management - NC Identity Management under the main menu item Application Services).

In consideration of this environment, describe the solution's capabilities to integrate with NCID. Also, explain the solution's capability to externalize NCID. Within Section IV. Cost Proposal, include an estimate to integrate NCID with the proposed solution understanding that this is a decentralized solution and will be invoiced by the individual agencies.

Enterprises seeking a tighter access control mechanism can enable SAML SSO to centrally manage their Sign account users through the corporate identity system. Adobe Document Cloud Sign services can be configured and integrated with identity management services that are SAML based.

For signers being authenticated using NCID, Sign will still go through a standard signing eSignature process of validating via email address or other Sign specific signer authentication options (password, 2-factor, KBA). Adobe has no dependency on any external identity authentication for the signing process.

Adobe Sign's API can be used to execute Sign services after going through third party authentication like NCID.

Please also address the following:

- a) Describe how the solution handles varying roles for authorization. Such as guest account (citizen non-authenticated), administrators, etc.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These roles and permissions allows State of NC to create different user accounts with varying roles of authorization like guest account, administrators, etc.

- b) The state seeks to achieve reduced or simplified sign-on capabilities. Describe how the solution supports reduced or simplified sign-on.

State of NC can enable Security Assertion Markup Language (SAML) SSO to manage Adobe Sign users through your corporate identity system. Adobe Sign, acting as the service provider (SP), supports single sign-on through SAML using external identity providers (IdPs) such as NCID, Okta, OneLogin, Oracle Federated Identity (OIF), and Microsoft Active Directory Federation Service. Adobe Sign is compatible with all external IdPs that support SAML 2.0.

- c) It is possible that there will exist multiple identity stores or vaults. Explain the solution's capacity to handle federated identity.

Yes, it is possible that there will exist multiple identity stores or vaults. Adobe uses an underlying identity management system to authenticate and authorize users. If you're using named licensing or are planning to provide access to services, using identities is a requirement. Adobe supports three identity or account types; they use an email address as the user name.

Adobe ID is created, owned, and managed by the end user. Adobe performs the authentication and the end user manages the identity. Users retain complete control over files and data associated with their ID. Users can purchase additional products and services from Adobe.

Admins invite users to join the organization, and can remove them. However, users cannot be locked out from their Adobe ID accounts. The admin can't delete or take over the accounts. No setup is necessary before you can start using Adobe IDs.

Enterprise ID is created, owned, and managed by an organization. Adobe hosts the Enterprise ID and performs authentication, but the organization maintains the Enterprise ID. End users cannot sign up and create an Enterprise ID, nor can they sign up for additional products and services from Adobe using an Enterprise ID.

Admins create an Enterprise ID and issue it to a user. Admins can revoke access to products and services by taking over the account, or deleting the Enterprise ID to permanently block access to associated data.

Federated ID is created and owned by an organization, and linked to the enterprise directory via federation. The organization manages credentials and processes Single Sign-On via a SAML2 Identity Provider (IdP).

Adobe recommends Federated IDs for the following requirements:

- To provision users based on your organization's enterprise directory.
- To manage authentication of users.
- To maintain strict control over apps and services available to a user.
- To allow users to use the same email address to sign up for an Adobe ID.
- In all K-12 user settings to ensure compliance with student privacy and other relevant laws

7) Architecture

The state prefers a cloud-based, software as a service (SaaS) solution; therefore, please address the following:

a) What is the solution's SaaS architecture model?

The SaaS architecture model can be found on the Adobe Sign Technical Overview document, found in Adobe Sign's SaaS architecture model.

- *Please refer to Attachment J for the Technical Overview.*

b) Provide examples of scalability for very large organizations and numbers of concurrent and daily transactions.

Adobe sign is highly scalable. We will be constantly monitoring use, to scale ahead of use requirements. Adobe Sign has many large customers sending a significant volume of transactions daily and annually. By partnering with a world class provider, AWS, we ensure a platform that can scale immediately and automatically whenever necessary, considering costs. All the data is stored at the cloud servers, with practically unlimited storage, so State of NC can easily scale up to as many documents as they need. This can be extended to all lines of businesses and regions State of NC caters to.

The exact count of concurrent and daily transactions is not disclosed, but over 6 billion electronic and digital signature transactions are processed through Adobe Document Cloud each year.

- c) Describe how the application performs under load, both in terms of number the number of users and the transaction volume.

As mentioned in above response, Adobe Sign is highly scalable and performs well under load. There is no practical limit to the number of concurrent users that can use the application at the same time. Similarly, there is no practical limit to the number of transactions which can flow through the Adobe Sign application for a implementation. Overall, over 6 billion electronic and digital signature transactions are processed through Adobe Document Cloud each year.

- d) Does the application dynamically scale based on runtime usage and demand?

No. However, we will be constantly monitoring use, to scale ahead of use requirements whenever it is required.

- e) Provide details to further demonstrate that the proposed architecture and supported platform will scale to meet State current peak and future application processing and user demand.

Adobe sign is highly scalable. The Adobe Sign architecture is designed to scale and handle large volumes of transactions without performance degradation. To provide a high level of availability and scalability, all Adobe Sign transactional data is stored in multiple distributed redundant database clusters with automatic failover and recovery. Adobe has the capacity to support large enterprise customers. The web servers distribute complex dynamic requests to the Adobe Sign application servers in the business layer through the use of load balancers.

- f) Describe the proposed solution's applications architecture, including offline capabilities, multi-language support, and interface standard supported.

Please refer to Adobe Sign Technical Overview document for Adobe Sign's SaaS architecture model.

- *Please refer to Attachment J for the Technical Overview.*

Anyone can quickly and easily sign a contract wherever they are, even executing it offline if Internet access is unavailable. On iOS devices, you can even sign documents offline. The app syncs automatically when you're back online.

At the Global level account, signers can execute contracts in their native language, and senders can choose from 34 languages. Adobe Sign Global supports English, German, Chinese, Japanese, Korean, French, Spanish, Italian, Dutch, and more.

- *Please refer to Attachment L.*

Adobe Sign is a 100% browser based system and can run on any device with browser support. Please visit <https://helpx.adobe.com/sign/system-requirements.html> for a complete listing of the minimum system requirements.

- g) Describe the solution as related to smart devices and operations on smart devices including but not limited to smart pads, smart phones on various platforms. Include limitations in functionality, security, need for installation of facilitating software (apps) and possible additional costs.

Adobe provides both a Web and Mobile solution. The application can be used to request signatures from others using a browser or mobile device. Your signers just click a link to open and e-sign from any connected device, be it a mobile phone, tablet, kiosk, signature pad or any other mode of technology which involves a hardware to sign and a web browser (or HTML) support. No signups or downloads required. The State of NC employee or agent can leverage

both the web and mobile applications via the same user account. There is no need to have separate accounts or login credentials to leverage either application.

Our iOS and Android Adobe Sign mobile applications serves to enhance the Adobe Sign product by providing specific functionality that extends the system's capabilities and convenience.

The mobile application allows the user to log in to their account and

- Send documents to sign
- Open and sign documents
- Sign directly on the screen
- Sign documents off-line
- Get signatures in person when meeting with a client
- Access documents from Google Drive, Box, Dropbox or Adobe Document Cloud
- View and manage the documents you have out of signature

The web interface for Adobe Sign services is a responsive interface which scales appropriately for smartphone, tablet, and computer screens. Adobe Sign also provides native support for a variety of mobile devices for both senders and signers. State of NC users may also prepare and sign documents through a touch-friendly interface on a mobile web browser (browser must support HTML5). Adobe Sign Services functionality is identical on desktop and mobile devices when accessed through a web browser. Also, there are no Security limitations on mobile devices compared to desktops. All the security provisions/features will be identical for both desktop and mobile devices.

8) Interoperability and Integration

The proposed solution may be required to interface with a variety of other systems. In consideration of this need, respond to the following:

- a) Please describe in detail what type of integration the solution supports; i.e., the integration architecture.

Adobe Sign offers great Integration capabilities with existing business systems and associated data stores. The State of NC users can use pre-built integrations and APIs to embed e-signature processes into enterprise applications, such as Salesforce, Workday, and Microsoft SharePoint (online and on-prem), and Dynamics CRM. The integrations are easily added to the 3rd party systems. Adobe Sign can be easily added to State of NC's business applications using comprehensive set of REST APIs.

Adobe also provides turn-key integrations into a number of contract management and document management systems including Apttus, SAP Ariba, SAP CLM, Selectica (Determine), Determine, Microsoft SharePoint, Box, ASC, IBM Emptoris, Intelligent Contract, McKesson, Oracle, Revitas, SciQuest, SpringCM, Salesforce Steelbrick, Dropbox, and many others.

- *A full listing is available by referring to Attachment M .*

For applications not listed above, Adobe provides many other easy methods for integration, including email to specified watched mailboxes, download into watch folders (which is supported by some systems), as well as a set of APIs for integration.

- b) Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided. Some of the potential integrations are:

Adobe Sign leverages REST, SOAP and Java API to allow customers to gain access to the wide breath of features and functionally within the application. Many of our clients leverage these API to develop both desktop and mobile applications. These APIs can be leveraged to fetch data from the back end systems, as well as write data back into them. As a State of NC developer, you can build a variety of integrations with Adobe Sign using just the APIs. Once built, integrations allow you to start the Adobe Sign signing experience entirely from within the external application.

- *Please visit Attachment N for complete API documentation.*

- i) SAP (SAP SSO cookies for example)

Please refer to the response provided against requirement number 8(a)

- ii) Web services (MQ Series, other APIs)

Please refer to the response provided against requirement number 8(a)

- iii) Enterprise Service Bus (e.g. Web Sphere Service Broker)

Please refer to the response provided against requirement number 8(a)

- iv) LDAP (for authentication)

Please refer to the response provided against requirement number 8(a)

- v) NCID (for identity management)

Please refer to the response provided against requirement number 8(a)

- vi) Document management systems (list)

Please refer to the response provided against requirement number 8(a)

- vii) Office software packages (Office 365)

Please refer to the response provided against requirement number 8(a)

- viii) Business systems such as human resources, accounting, finance, CRM, ERP, LMS, etc.

Please refer to the response provided against requirement number 8(a)

- ix) SharePoint Online and On Premises

Please refer to the response provided against requirement number 8(a)

- x) Dynamics 365, Salesforce.com

Please refer to the response provided against requirement number 8(a)

- c) Are APIs secure and encrypted? What Encryption Method,

Yes. All API data is encrypted in-transit and at rest using AES encryption over HTTPS using TLS 1.2.

- d) How do you extract form or record data? Do you use industry standards such as XML?

Adobe Sign APIs leverage JSON format for responses of the events fired by Adobe Sign. CSV format is used to extract data from the application when an external application calls, for

example, to retrieve the data filled by the users at the time of signing the Adobe Sign widget in the external application. REST APIs can also be made to accept XML payload as the input.

- e) How is data inserted into a form? Can data be inserted dynamically (based on user inserted data)?

It is easy to insert data into a form. User can click on any Form field (Text field, Signature field, etc.) and enter the respective data over there from desktop or mobile. Also, data can be inserted dynamically in form fields depending on user inserted data in the previous form fields. This can be done by setting conditions for the respective form fields.

- f) Can forms be processed via API in both real time and/or batch mode?

Yes, forms can be processed via APIs in both real time and/or batch mode.

Some form fields can be pre-fetched from databases, external applications, etc. External applications can also receive status updates in real-time for form transactions initiated using Adobe Sign.

- g) How does the API deal with multiple accounts (for enterprise-wide forms)?

Adobe Sign APIs allow for permissions to be defined for specific permissions and user scopes to ensure APIs only access appropriate information.

- h) Can the API retrieve software version numbers?

Please see API documentation by referencing N.

- i) How are fields identified in the API?

Please see API documentation by referencing N.

- j) How is the workflow engine capable of easily supporting a variety of e-forms?

A variety of e-forms can be created through workflow engine by placing variety of form fields and different types of documents/e-forms (like parallel signing, sequential signing, mix) can be sent to different signers using the extensive workflow capabilities.

- k) The state prefers REST web service interfaces. XML schemas should be derived from industry standard vocabularies where possible such as the National Information Exchange Model (NIEM). Describe how the solution will support these and other interoperability standards.

Adobe does use industry standard REST Web Services to programmatically interact with the Adobe Sign services. Adobe Sign does not conform to the NIEM schema specification.

- *Please see API documentation by referencing N.*

9) Applications Management and Control

Describe the process of raising and managing exceptions within the application. Please include the following:

- a) Address whether multifactor authentication (MFA) access is available for all accounts including signatories, admins, and form builders? Is it included in the price? If not provide pricing in the cost section.

Yes, Adobe Sign provides a number of second factor identity verification methods (Signing password, Phone verification, etc) that can be used to verify a signer's identity.

It also supports two factor authentications (MFA) for admins, form builders, etc. Generally, this is handled by the IDP (e.g., Okta, OneLogin, Oracle Federated Identity (OIF), and Microsoft

Active Directory Federation Service), and Adobe Sign integrates with this via the out of the box SAML capability.

MFA is available for is available for all users. Prices for MFA are included in the cost section.

- b) Describe the level of customer control on the timing of applying patches, upgrades, and changes to the SaaS application and the notification process to be used.

Through their Account Manager about the upcoming changes. Adobe Sign updates are automatically applied for all customers. For new functionality, customers are notified prior to release and given the option to opt-in to new features.

Most maintenance and release upgrades require no downtime. Scheduled maintenance that required downtime will usually take place on Saturdays between 10:00 PM to midnight Pacific Standard Time. In case the application needs to be taken down for maintenance, customers are notified in advance regarding when the service is expected to be unavailable.

- c) Explain the process for handling software defects.

Adobe will provide Phone support available 24/7 for all the clients under active contract to handle software defects and any service disruptions. Adobe maintains a dedicated geographically dispersed team of technical operations engineers utilizing a “follow-the-sun” model where working hours are allocated during regular business hours. This global team provides 24x7x365 on-call response support to assist the corporate Adobe incident response team with resolving software defects and any disruption to the service as quickly as possible.

Also, State of NC can reach out to their Account Manager or Customer Success Manager for any immediate assistance to handle software defects.

- d) Describe the major and minor release policy for the solution.

There are 3-4 minor releases per year and a major release in every 12 months. Updates and new releases are included during the time in which the agreement is in force.

- e) Describe user configuration capabilities.

The Adobe Sign User Interface is highly configurable. Users may configure templates, notification settings, create and edit workflows, add State of NC branding to Adobe Sign, upload and save their signatures for convenient signing, and more. You may also configure/modify how long documents are kept in the solution after they are signed. Adobe Sign was built with flexibility in mind.

State of NC users have several options for customizing the Adobe Sign interface. Customers can add their own logo and color branding that in turn will display during the signing experience. Another option is to leverage the Adobe Sign API's. By using the API, can embed the signing experiences within the State of NC web or mobile application.

- f) Describe user self-provisioning capabilities.

State of NC will be assigned with onboarding specialist who will help in provisioning of software. You can also leverage Adobe Sign Admin guide for self-provisioning.

- *The Admin Guide is available by viewing Attachment O.*

- g) Describe the level and skill set needed by the State to administer and configure the proposed solution.

Adobe Sign is a browser-based solution and running the application is just like opening and using a website. State of NC business users can administer and configure the solution themselves without coding or without being a technical expert.

h) How do you address Delegation of authority?

A sender can specify a delegator role while preparing the document for signature in Adobe Sign. The delegator will receive an email request for the final signer's email address. Signers can also elect to delegate to another person if desired. All delegations are recorded in the audit trail for a document.

i) Describe how privileged management accounts are secured, provide encrypted authentication and access to authorized users.

Adobe Sign uses a role-based model for identity management that handles authentication, authorization, and access control throughout the Adobe Sign system. Capability-based security and authentication processes are defined and enabled for an organization by an Adobe Sign administrator. This ensures that only authorized users can view or modify the document as per their user responsibilities, and only authorized users have access to the document.

By default, only the sender of a document has access to their own documents.

Adobe Sign provides an user-account sharing mechanism which allows granular access to the documents of other users. Options include (View, Manage, Delete, Send As)

- *For more details on authentication, please refer the sub-section "User Access Security" in the Admin Guide, Attachment O.*
- j) Specifically, does the Delegation of Authority capability that allows signatories to delegate signing authority for documents for a specified period of time, or indefinitely.

Users can establish delegation to other users for an indefinite period of time. If not needed anymore, delegation can be deactivated.

10) Application Specifications

Please describe how the solution will include the following application specifications:

a) Describe integration with Microsoft Office 365 Office Productivity & Email.

With Adobe Sign now in all your Microsoft Office 365 apps, it's easier than ever to get e-signatures right from the solutions you use every day. With Adobe Sign and Microsoft Office integration, the users can easily convert Microsoft Office documents into PDF files from within Office applications, and apply a password to restrict access. Adobe Sign supports Microsoft Word (.doc and .docx), Microsoft Excel (.xls and .xlsx) and Microsoft PowerPoint (.ppt and .pptx). The senders can also automatically generate form fields with PDF forms or within Microsoft Word by using document tags to help ensure consistent data and repeatable processes. Moreover, Adobe Sign works seamlessly with Microsoft Dynamics CRM to help you close deals faster, reduce risks, and increase retention. You can integrate without any coding, so you'll get up and running in no time. The application runs on all Microsoft windows operating systems and the documents are supported for printing as well.

- *Please see the attachment AB for White Pages on Microsoft Office 365 integration.*

Additionally, this is supported in Adobe Sign solution by leveraging the Outlook add-in. The Adobe Sign for Outlook add-in allows a user to configure a new agreement from within their email client by either composing a new email, starting from a blank slate, or by replying to an existing email, importing the recipient list, and automatically attaching any files from the source

email. The Adobe Sign for Outlook add-in can be installed in both the web based and desktop launched applications. Installing the application in one environment enables it in both.

- *For more details, please refer to Attachment P.*
- b) Describe how the solution can initiate the signature process with PDF and Word documents. *Please note that the vendor may apply custom branding (official logos, colors, hyperlinks) as necessary to create a consistent user experience. Please see [Section III, #6](#) for more information.*

The Adobe Sign interface is intuitive both for those who send documents and those who sign them, with minimal instruction needed to prepare documents for signature. A single click initiates a document and signature workflow. Workflow Designer lets you create easy-to-follow “send” experiences for your users so process steps can be followed consistently every time. With this tool, administrators can design and manage workflow templates easily with an intuitive drag-and-drop editor. It's easy to specify: documents to be included in an agreement; characteristics of the participants, including predefined names and roles; form fields to be pre-filled by the sender; agreement expiration or password options; and more.

For consistent user experience, Adobe Sign provides the ability to brand the signing experience to the look and feel of State of NC. Signers will have confidence that they are interacting with State of NC and are not presented with logos, agreement to terms, or other intrusions from the signature vendor.

State of NC can apply its corporate branding in several different ways. The Adobe Sign web site can be branded with your organizations logo. You even have the option to completely remove any Adobe company branding from the interface, emails and web pages. Email communications sent from Adobe Sign may be customized with your graphics in the header and footer. Additionally, you have the option to customize the textual content of the emails in various ways.

During the signing experience, the signing page can be modified to contain your custom graphics customization within the header and footer area. Next, external emails sent to signers are branded at the account or group level. When the signer receives the e-mail, it is very clear that the email is coming from State of NC and not Adobe.

Finally, after the customer has signed the document, you have the option to redirect the browser from the standard Adobe Sign “You have completed Signing” page to a customer-specified landing page where you have complete control of branding and appearance, rather than a landing page full of our company’s logos and promotions.

Adobe prioritizes the experience of your signers. Adobe Sign can be branded to suit your audience and shape the signer experience. For example, notification emails can be fully customized with your own verbiage, colors, and logos.

- c) Describe how the solution works with Section 508 compliant screen readers and other ADA capabilities. Specifically, in- process and completed documents should be fully read by a screen reader.

Adobe is committed to accessibility and strives to address it in its products and services. U.S. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

- *Adobe Sign features that support accessibility for people with disabilities are summarized in Attachment Q.*

- d) Provides a digital signature solution in which the "root" digital certificate is provided by a certificate authority that meets assurance and trust requirements by Adobe. Documents with these certificates become automatically trusted by Adobe as this facilitates the ability to validate the signature. More information about Adobe's Approved Trust List and current members of that list can be found at <http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>.

Yes, after all the parties have signed the document it is certified with AATL (Adobe Approved Trust List), which is one of the services enabled by the Adobe root certificate authority (CA) and then stored encrypted on the file system. The AATL enables PDF documents to be signed using a standard digital certificate. These documents are automatically validated when viewed using Acrobat or free Acrobat Reader. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed. Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

The AATL enables Acrobat and Acrobat Reader to trust the integrity of e-signed documents. Adobe stores the key that is used to sign the document in a hardware security module to prevent online attacks and tampering.

- e) Provides the ability for anyone to open a digitally signed PDF and observe a signature validity confirmation across the top of the file that indicates all signatures are signed and valid.

The final signed PDF document is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

- f) Users of the e-signature service are given an opportunity to decline to use the service.

Yes, while signing, a signer can choose to decline the document. To do this, in the signing process, the signer just needs to select "Options" and select "I will not e-sign/approve" to decline the agreement. The same is recorded in the audit trail as well. In the condition that the signer declines to sign, the reason for declining will be asked to the signer, and the workflow will route the document back to the sender. The sender can make changes and send the document again for signature, or can cancel the transaction altogether.

- g) Does the solution provide the capability for electronic notarization.

There is no reason why a Notary could not be included in a signing workflow; however, this specific persona is not supported. The deployment of eNotary solutions is an evolving landscape, with varying legal requirement across States and the US. Adobe has a multi-

threaded approach to providing eNotary solutions; Adobe will partner to provide remote electronic notarial requirements identified by the State of North Carolina. Our partnerships allow us to provide a host of flexible approaches and options; together with our partners, we enable the enterprise management of the entire electronic notarial process including the notary and signer profiles.

Option 1: Technology Infrastructure A digital cloud solution for remote electronic notarial requirements that incorporates, Electronic Signature and Video CAM technology to allow for a total digital transaction end to end, and with full return. Under this scenario, Adobe assumes Georgia State Lottery Corporation will provide the physical notaries.

Option 2: Services & Technology Infrastructure (Includes everything in Option 1) This option anticipates including and managing nationwide notary/attorney fulfillment. While Adobe's focus is online and authenticated signing, we can partner with the leading notary services organizations to provide complete document signing fulfillment, from scheduling to oversight and return. Accommodating wet signed or electronically notarized office/at home or notarized online, we can accommodate all the signing requirements identified in the RFP.

- h) Digital signature notifications are achievable through SMTP relay, direct email client integration (i.e. "mailto:"), or SMS (text messages). Please describe these and/or other capabilities.

Adobe Sign solution sends digital signature notifications through SMTP relay. However, State of NC can use APIs to integrate with third party email clients to send digital signature notifications.

- i) Describe what notifications are sent to a user for signature?

Adobe Sign uses email for signature event notifications to senders. Notifications are available for the following events:

- When a document is viewed
- When a document is sent
- When a document is signed or approved
- When a document is declined
- When a document is forwarded
- When a document is uploaded by a sender
- When an agreement is expired
- When an email is bounced
- When a document is not viewed in a specified time
- When a document is not signed or approved in a specified time
- When a document is viewed but not signed in a specified time
- When a document will expire

Also, Adobe Sign lets the senders set a reminder for a transaction. They're used to remind signers they have a document that is waiting for them. They are sent in the form of emails and can be sent at certain intervals. The reminder can be set as the transaction is being sent, and also on a transaction which was sent earlier. The sender has the ability to configure who you want to remind, the frequency of the reminder, and a note to include in the reminder email. The sender can also cancel a reminder.

- j) Please describe the solution's policy for handling customer's intellectual property, data, and information.

Backed by more than a thousand security features, processes, and controls, Adobe Sign is certified compliant with the industry's most rigorous security standards, including SOC 2 Type 2, ISO 27001, and PCI DSS used in the Payment Card Industry. Adobe Sign complies with industry-specific regulatory requirements, such as HIPAA, FERPA, GLBA, and the Food and

Drug Administration (FDA) 21 CFR Part 11 regulation in the United States. Additionally, Adobe Document Cloud Adobe Sign services managed data center is audited annually to ensure that it meets or exceeds SSAE 16 Type II SOC 2 requirements. The Statement on Standards for Attestation Engagements (SSAE) No. 16 measures the controls relevant to financial reporting, and the Service Organization Controls 2 (SOC 2) measures the IT controls of security and availability.

- *Additional information can be found by viewing the Compliance Overview, found in Attachment I.*

- k) Describe if the solution can import a predefined electronic list (i.e. CSV, ODBC, Excel) of customer's vendors and business partners. Please describe capability and any limitations that may exist.

You can use a CSV file to import your recipients' email addresses and merge custom data into fields on the document for each recipient.

.CSV stands for Comma-Separated Value and Excel files can be saved in this format.

11) Automation of Forms

Explain how the solution will address the automation of forms. Provide an explanation regarding the:

- a) Process for integrating field validation (both data and format).

State of NC can set up Agreement form fields to allow that only a specific format of data can be entered.

By default, a form field allows any combination of letters, numbers, or special characters:

`~!@#\$%^&*()_+ -=[]\{}|;':",./<>?£

Use validation if you want to only allow the entry of a specific format of data in the field. If the validation is not passed, the form will display a red warning balloon and also the form cannot be e-signed until the field is validated.

In the drag-and-drop authoring environment, you set the validation for a field by double-clicking the field and choosing an option from the Validation list.

- *For more details, please refer to Attachment R.*

- b) Process for database integration.

Given that the Adobe Sign system is provided as a SaaS based solution, the client has no requirement to provide or manage or integrate with the database underlying that Adobe Sign solution. Additionally, all calls to access information from the Adobe Sign system occurs via the Adobe Sign API, making data access transparent to the client.

- c) The limitations on the number of standard templates that can exist.

Adobe Sign provides a few standard templates upon implementation of solution. The users can use these existing templates, modify them to include signature fields and use them as templates for future signature requirements. This document can then be added as a template to the library and used any number of times to collect signatures from multiple users. Hence, users can create any number of templates and save them in library for future use.

- d) Level at which standard templates exist – whole org., division, etc? Provide examples.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These roles and permissions allow State of NC user groups to access only the templates which are assigned to that concerned user group. Hence, whole org., can access particular set of templates and a particular division of user group can access only specific templates for which they got assigned to.

- e) Revision process to forms without customization from vendor.

Yes, forms can be revised without any customization from vendor with the help of easy-to-use drag and drop editor. You can drag and drop form fields on to a form/template for revision purposes.

- f) Use of existing form templates created by other products.

State of NC can import or upload documents created by other products and save them as templates in Adobe Sign solution for future reuse. Adobe PDF's with Form fields are automatically mapped 1:1 with Sign fields. Adobe Sign can also use AI techniques to do form field recognition based on form text and boxes.

- g) Methodology regarding how calculations are conducted within form.

Please refer the sections "Custom - Regular Expression" and "Custom - Formula" in Attachment R.

- h) Process for creating and publishing forms to agency websites.

When documents are signed, they will be saved in Adobe Sign solution. State of NC can use custom APIs to fetch these documents and publish them to agency websites.

- i) Process required for citizens to use forms posted to Agency websites via the solution.

This is part of the self-service offering of Adobe Sign and is as easy as downloading a form but with the added benefit of an interactive self-service session. The website would have a URL link that the citizen would click on and in that session the signing ceremony being managed by Adobe Sign would be displayed. The user then interacts with the form and when completed, they would verify their email address and be able to download a copy of the signed form. These self-service forms are referred to as widgets in Adobe Sign.

- j) Methodology regarding how persons in a workflow can redline data in a form that is in process and route that form back to the originator for revision. Describe the form data capture – stored in form replica and/or recreated from database and ability to extract either way.

Adobe Sign is meant to be used as part of the final step in an agreement process and therefore no revisions or mark-up are allowed. If a signer does not agree with the content, they can refuse to sign and can follow-up with email on reasons. In addition, a form can be configured to allow for dis-approve options along with comments a signer can complete. All data entered in a form is saved in the system and can be exported by a user or via APIs.

- k) Process for pre-populating user specific information such as name, address, and etc.

Via API integration, some fields can be pre-fetched into forms from databases, external applications, etc. Other options include being able to directly pre-populate from SharePoint data

lists, pre-populate from other integrations such as MS Dynamics and Salesforce, and using MegaSign for batch signing and pre-populating from a CSV file.

- l) Solution's method for marking sections of the document where signature is required.

Using Adobe Sign's document editor, we can drag and drop signature fields to the document and specify where end user needs to sign.

- m) Solution will allow forms to be labeled by type of process, such as HR, Finance, Payroll, etc.

Yes. Using Adobe Sign's document editor, we can place label fields on documents specifying HR, Finance, Payroll, etc.

12) Workflow

Describe the solution's workflow capabilities. Include the functionalities below within the description:

- a) Provide examples of templates for developing workflows per the solution that will standardize business engineering processes and improve workflow development efficiency.

Adobe Sign helps an organization replace paper-and-ink signature processes with 100% digital workflows. Adobe Sign offers workflow customization solutions that span the full range of touchpoints, letting you automate signature processes and speed business across your entire organization. Adobe offers two powerful and easy-to-use options that let administrators or business analysts customize signing workflows for their organization — with no “coding” required.

Workflow Designer lets you create easy-to-follow “send” experiences for your users so process steps can be followed consistently every time. With this tool, administrators can design and manage workflow templates easily with an intuitive drag-and-drop editor. It's easy to specify: documents to be included in an agreement; characteristics of the participants, including predefined names and roles; form fields to be pre-filled by the sender; agreement expiration or password options; and more.

As previously mentioned, Adobe Sign has out of box integrations with other workflow-based products such as Adobe AEM Forms, Nintex and Thinksmart. These allow more advanced workflow concepts such as dynamic routing and advanced form business logic to be utilized.

- b) Any limitations to the size of documents sent through workflow.

The default limit is set at 10MB by default but we can increase this to meet your requirements.

- c) Any limitations to the combined file size of a transaction with multiple files attached.

The default limit for Signer attachments is 25 pages and 5 MB but this can be increased via customer support approval.

- d) Each person in the workflow is given the opportunity to review all documents, with a confirmation opportunity, before the transaction continues.

Yes. Each person in the workflow can be assigned as reviewer, with a confirmation opportunity, before the transaction continues.

- e) The solution allows for rejection. If a form is rejected, specify how commenting, rerouting, markup of document is allowed.

Yes, the Adobe Sign workflows allow the reviewer to add comments to the document and send it to the initiator for taking actions.

Similarly, the signer, during the signature ceremony can choose not to sign, and send the initiator/sender with a message mentioning the reason for rejection. The sender can make changes and send the document again for signature, or can cancel the transaction altogether.

- f) The solution supports the approving/rejecting of multiple sections of a document by more than one approver and/or signer.

Yes, the solution supports the approving/rejecting of multiple sections of a document by more than one approver and/or signer.

- g) Workflows are setup based on Roles and Permissions

Yes, workflows can be setup based on roles and permissions. This is achievable through Adobe Sign's Workflow designer. While designing the workflow, in the Recipients Routing section, you can specify the recipients and the routing order per your requirements. It also allows the State of NC users to select the role (signer or approver or viewer) you want to insert.

- *Please refer to Attachment S for more details.*

- h) User initiates signing.

Yes, once sender sends the document to the signer/user via email, signer can click on the link in email and initiate the signing process.

- i) Each department/division/unit can have and maintain their own customizable workflows.

Yes, each department/division/unit can have and maintain their own customizable workflows.

The Adobe Sign security model is user role based with access grants to support granular-level functional and data level security. Standard roles and permissions are provided with our standard implementation and additional roles can be defined / modified as needed by State of NC. These roles and permissions allow State of NC departments/divisions/units to have and maintain their own customizable workflows.

- j) Routing of multiple types of documents with multiple signatures within a single transaction.

Yes, Adobe Sign provides extensive workflow capabilities allowing for agreements to be signed in a particular sequence. In such a case, separate emails are sent to each signer in the sequence that is required to sign the agreement. The sender just needs to enter the number specifying the order of receiving documents by each signer as shown below:



- k) Users can track the progress of a transaction – including stage and status.

Yes, Adobe Sign allows users to monitor the status and progress of agreements in real time, alerts and email notifications. A detailed audit trail that lists all events and actions taken by the participants is stored together with the agreement. This can be done by navigating to the Manage Tab of the Adobe Sign interface, selecting the agreement for which audit trail is required, and viewing the detailed audit trail from the History tab. CenturyLink users can also

run a report on transactions sent from users in the account. You can also export a CSV file with the raw data generated from the report.

The documents are categorized on the Manage page and all agreements are sorted into these various sections. You can filter by status and you can also search by status.

- l) The process for copying previously created workflows

State of NC users can save previously created workflows as templates in the library and reuse or copy them whenever required.

- m) The solution generates a diagram of the workflow.

Yes, Adobe Sign solution generates a diagram of the workflow.

- n) User can abandon signing a document.

Yes, the signer during the signature ceremony can choose not to sign and send the initiator with a message mentioning the reason for rejection. The sender can make changes and send the document again for signature, or can cancel the transaction altogether.

- o) Portions of the workflow that are configurable by the Department/Division/Unit.

Based on permissions of the author, entire workflow can be configurable.

- p) Queues are established to assist users to process, review, analyze and approve depending on role.

These are typical options that integrated third party workflow tools can provide and use to determine the Adobe Sign routing process.

- q) Support Ad Hoc signing from cloud and smart devices.

Yes, Adobe Sign solution supports ad-hoc signing from cloud and smart devices.

- r) Workflow creation can be automated. (i.e. – Roles copied from other systems such as HR/Payroll systems).

Yes, workflow creation can be automated. Workflows can be defined via API.

- s) Documents which do not require signature are bound to signature documents and routed through the workflow.

Yes, documents which do not require signature are bound to signature documents and routed through the workflow.

- t) Workflow can be redirected and users injected to the flow.

Yes. A sender can specify a delegator role while preparing the document for signature in Adobe Sign. The delegator will receive an email request for the final signer's email address. In this way, workflow can be redirected and users can be injected to the flow. Signers can also elect to delegate to another person if desired. All delegations are recorded in the audit trail for a document.

- u) Support branding and color scheme customization of document packages for signature.

Adobe Sign provides the ability to brand the signing experience to the look and feel of State of NC. Signers will have confidence that they are interacting with State of NC and are not presented with logos, agreement to terms, or other intrusions from the signature vendor.

State of NC can apply its corporate branding in several different ways. The Adobe Sign web site can be branded with your organizations logo. You even have the option to completely remove any Adobe company branding from the interface, emails and web pages. Email communications

sent from Adobe Sign may be customized with your graphics in the header and footer. Additionally, you have the option to customize the textual content of the emails in various ways.

During the signing experience, the signing page can be modified to contain your custom graphics customization within the header and footer area. Next, external emails sent to signers are branded at the account or group level. When the signer receives the e-mail, it is very clear that the email is coming from State of NC and not Adobe.

- v) Support document creator workflow rerouting with and without workflow start over.

Options for a sender to re-route or re-start a workflow does not have technical limitations but have limitations due to legal constraints with eSignatures, unlike typical workflow functions. For example, a sender can replace email recipients, esp. if one is not available but cannot change routing or once it has been signed by a signer. In addition, content cannot be changed while the transaction is in process, especially one it has been signed by at least one recipient.

- w) How an external system process can be added as a workflow step/approval.

Adobe Sign's workflow engine is built for defining user-controlled steps as part of an Adobe Sign transaction. Typically, Adobe Sign is incorporated into another third-party workflow engine rather than having a system integration as a workflow step within Adobe Sign.

- x) Describe how the solution will generate workflow and forms meta-data and the content of such meta-data specifying what is included, and what is excluded.

Adobe Sign creates workflows by default using the Workflow Designer: *(Please refer to Attachment S)*. These can also be created via API.

For every document that is sent through Adobe Sign, a corresponding audit report logs this history of that document, including when it has been sent, viewed, signed, approved, identity verification has been established, and how they recipient signed. Each event is also tracked with their name, email address, IP address, date and time. Adobe Sign audit reports are stored in perpetuity as an encrypted and certified. Audit reports can be downloaded as a certified PDF from Adobe Sign at any time, which can also be appended to the agreement, or made available by clicking on any of the signature images in the document. The intent of the audit report is to provide a history of the document.

- *For a full list of the metadata that can be collected related to a transaction, see Attachment S.*

13) Signature/Initialing

Describe the solution's signature and initialing capabilities. Include how the:

- a) Digital signature is linked to the documents being signed. Describe how this is achieved.

Yes. Once signer signs the document, signature will be automatically embedded in the document by our solution itself.

- b) Solution assigns and restricts the sole control of the signature to the owner.

The document viewing and signing process is conducted entirely within a web browser via a secure, encrypted session. The "document" the client sees in the browser is a rendered version of the document pages, presented for viewing. The signer may only enter values or signatures into pre-designated fields whose content is delivered back to the Adobe Sign server and merged

into the master, certified PDF document. The signer is never in complete control of the document.

- c) Solution captures the users "actual" signature and initials.

Yes, Adobe Sign solution can capture the users actual signature and initials using touch devices (i.e. mobile, tablets, etc.). There is also an option to 'draw' a user's signature with a mouse.

- d) Solution captures a picture of the signature owner and associates it with the actual signature.

Yes, Adobe Sign solution can capture a picture of the signature owner and associates it with the actual signature.

- *For more details, please refer to Attachment T.*

- e) Solution captures speed, pressure and x-y coordinates of signatures.

Adobe Sign provides multiple methods to capture an electronic signature including typed signature, drawn, signature image, and mobile signature. Mobile signature allows you to utilize your mobile device such as a smart phone as a portable signature pad via text message. Signature pads, which leverage digital certificates, can be supported using digital signatures through Adobe Acrobat Reader.

- f) Receiver of data can determine origin.

Adobe Sign can capture location coordinates from users of Adobe Sign mobile application.

- g) Electronic document cannot be altered without detection at any time after being signed.

During the Signing Ceremony, the participant is viewing a rasterized view of the document pages rendered in a web browser. the signer can only sign or fill in the specific parts of the document on which are assigned to them.

Following each signing session, the document is encrypted and certified on the Adobe Sign server.

The final PDF document is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

Each time the document is opened, a call is issued to VeriSign (assuming a web connection is available) updating the validity of the certificate and checksum of the document. If the document is found to have been altered in any way by bypassing the encryption, the document will display the status that the document no longer matches the certified checksum and is no longer a valid copy of the signed document.

- h) Code or other mechanism is used to create digital signatures and how that code or mechanism is unique to that individual at the time of signature.

Yes, code or other mechanism can be used to create digital signatures. This is possible through "Script-like font" signature style. This is the default value and the favored style currently. Adobe Sign applies a font to your name to achieve the appearance of a handwritten signature.

14) Repudiation

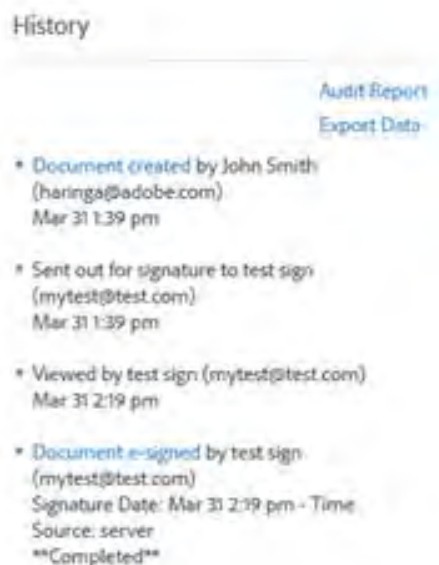
Describe how the solution addresses repudiation; specifically address how the solution will provide:

- a) True and correct copy of document received – provide sufficient evidence to show how the copy of record was derived from and accurately reflects the electronic document as it was received by the system, this evidence is also necessary to establish document integrity.

Adobe Sign provides necessary controls in-place to assist with non-repudiation including the identity of the signer, the integrity of the document, and the intent for the person to sign. All of this is tracked within the audit report. A signer's identity is verified based on the unique URL sent to their email address for signature. Additionally, two-factor identity verification can be used such as passwords, KBA, Social identity, Phone/SMS verification to verify the signer signing a document. At each stage in the workflow, Adobe Sign maintains a secure checksum of the document to ensure both document integrity and confidentiality. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents with a digital signature before distributing it to all participants. The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length cryptographically sound hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed. The intent of the signer to sign is built into the signing ceremony for a person to "click to sign" to verify their intent to sign a document. All of this is tracked within the audit report. Furthermore, Adobe Sign meets or exceeds the legal requirements for electronic signatures in many countries.

- b) A human-readable format that clearly and accurately associates all the information provided in electronic document with descriptions or labeling of the information and provides the opportunity to repudiate the electronic document based on this review.

For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time.



- c) Inclusion of other information necessary to record meaning of document – such as data field labels, signatory information such as references to validation mechanism, and transmission source information.

For every document that is sent through Adobe Sign, a corresponding audit report logs the history of that document, including when it was been sent, viewed, signed, approved, identity verification established, and how the recipient signed. Each event is also tracked with the name, email address, IP address, date and time. Audit reports are certified with a digital certificate to make them tamper-evident PDFs. These can be appended to the end of signed documents or downloaded at any time

- d) Procedures to address submitter/signatory repudiation of a copy of record.

Adobe Sign provides necessary controls in-place to assist with non-repudiation including the identity of the signer, the integrity of the document, and the intent for the person to sign. All of this is tracked within the audit report. A signer's identity is verified based on the unique URL sent to their email address for signature. Additionally, two-factor identity verification can be used such as passwords, KBA, Social identity, Phone/SMS verification to verify the signer signing a document. At each stage in the workflow, Adobe Sign maintains a secure checksum of the document to ensure both document integrity and confidentiality. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents with a digital signature before distributing it to all participants. The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length cryptographically sound hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity (see the following figure) and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed. The intent of the signer to sign is built into the signing ceremony for a person to "click to sign" to verify their intent to sign a document. All of this is tracked within the audit report. Furthermore, Adobe Sign meets or exceeds the legal requirements for electronic signatures in many countries.

- e) Confirmation of receipt of intact form data or record.

An audit document/record is created for each document which enters the Adobe Sign system and is resident on the server indefinitely as an encrypted VeriSign certified PDF file, ensuring its integrity.

Similarly, the final signed PDF document / Form data is locked and encrypted. Additionally, the document is certified by VeriSign, ensuring its integrity. When opened in Acrobat reader or Acrobat DC, the VeriSign seal is presented at the top of the page. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.

- f) Expunging of transaction upon authorized request.

Transactions (documents and meta-data) can be removed manually by account users and can be setup via written request to Adobe support to be removed automatically as part of the account purge process.

- g) Long term validation of electronically signed document. Describe how electronically signed document will maintain validity for long term (multiple years out).

All documents that are produced by Adobe Sign are LTV enabled for an unlimited period of time. All information that is needed to prove that the signature was valid at the time it was placed are integrated in the pdf document.

15) Notification

Describe the solution's notification capabilities, include if the solution:

- a) Provides opportunity to review certification statements and warnings (including any applicable certifications that false certification carries criminal penalties).

More information is needed.

- b) Provides notification that copy of record is available and this notification is configurable by each Department/Division/Unit.

Notifications content can be customized. Each department or individual can create message templates that will be used with each notification e-mail.

- c) Flags accidental submissions.

The Sender can cancel a 'accidental submission'/transaction and all parties will be notified of that cancellation and no longer will have access to the document(s).

- d) Supports setting expirations and notifications.

Adobe Sign uses email for signature event notifications. Notifications are available for the following events:

- When a document is viewed
- When a document is sent
- When a document is signed or approved
- When a document is declined
- When a document is forwarded
- When a document is uploaded by a sender
- When an agreement is expired
- When an email is bounced
- When a document is not viewed in a specified time
- When a document is not signed or approved in a specified time
- When a document is viewed but not signed in a specified time
- When a document will expire

You can customize your alerts using the Settings area on the portal. You can also have different settings for agreements sent directly to you and accounts that share information with you. The notifications and reminder can be automated as well as modified as per the need.

Also, Adobe Sign lets the senders set a reminder and expirations for a transaction. They're used to remind signers they have a document that is waiting for them. They are sent in the form of emails and can be sent at certain intervals. The reminder can be set as the transaction is being sent, and also on a transaction which was sent earlier. The sender has the ability to configure who you want to remind, the frequency of the reminder, and a note to include in the reminder email. The sender can also cancel a reminder.

- *For more details, please refer to Attachment U.*

- e) Has expirations and notifications that can be set for a standard (e.g. three-month expiry) for whole organization, a division, and individual and etc.

Yes, State of NC users can set custom reminders and notifications for a standard for whole organization, a division, an individual, etc.

- f) Makes it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory did not intend to be bound by – Finality function.

Yes, you can present users with disclosure option which makes it clear to them that the signed document represents a completed declaration of will. Adobe Sign allows you to add a consent clause to your agreements and a term of use for signers to agree to conduct business electronically. When a signer clicks the blue "click to sign" button during the signing ceremony they verify their intent to sign the document and accept the terms of use of the service. Record of this intent to sign the document is tracked in the audit report.

- g) Makes a signatory aware that by his/her signature he/she is entering into a binding transaction – Cautionary function.

Yes, you can present users with disclosure option which tells them that by his/her signature he/she is entering into a binding transaction. Adobe Sign allows you to add a consent clause to your agreements and a term of use for signers to agree to conduct business electronically. When a signer clicks the blue "click to sign" button during the signing ceremony they verify their intent to sign the document and accept the terms of use of the service. Record of this intent to sign the document is tracked in the audit report.

- h) Includes automatic acknowledgement of receipt.

Yes, when a document is viewed or signed by signer, sender will get an email notification as an acknowledgement.

16) Storage

Describe the following storage capabilities; include if the solutions storage functionality can:

- a) To print or store locally by person(s) in the process.

Yes, the final documents can be printed or stored locally by person(s) in the process.

- b) Form data or record will be stored – vendor or agency.

By default, the final signed documents are stored on the Document Cloud servers indefinitely. In addition, customers can request Adobe to remove documents permanently after x time. This purging is an automated process. Adobe also provides turn-key integrations into a number of State's own document management systems to store completed, digitally signed document(s). For example, Apttus, SAP Ariba, SAP CLM, Selectica (Determine), Determine, Microsoft SharePoint, Box, ASC, IBM Emptoris, Intelligent Contract, McKesson, Oracle, Revitas, SciQuest, SpringCM, Salesforce Steelbrick, Dropbox, and many others.

- c) Provide costs estimate for vendor storage in Section IV. Provide cost estimate for any transmission cost if stored at agency in Section IV.

There are no storage costs for documents stored in the Adobe Document Cloud nor are there transmission costs to download documents to Agency storage.

- d) Store and accommodate according to each department/division/unit record retention and disposition schedule.

Yes, Adobe Sign solution allows to store and accommodate documents according to each department/division/unit record retention and disposition schedule.

- e) Allow procedures for retrieving documents from Vendor; during contract term.

During contract term, Adobe Sign APIs can be used to retrieve signed documents.

- f) Allow procedures for retrieving documents from Vendor; expired contract term.

At the end of contract/service, the customer must call Adobe's Customer Support Center in order for Adobe to make the appropriate API calls to extract customer data. This data will then be placed into a file server that the customer has access to. The format will be either the original uploaded document format, or Certified PDF for signed documents. Audit trail information is retained indefinitely for regulatory compliance.

- g) Format documents are received and stored in.

Yes. Final signed documents are stored in PDF format on the Document Cloud servers indefinitely.

- h) Support document package labeling for ease of segmented document storage outside of the native solution datacenter

All documents from Adobe Sign are returned as a certified tamper-evident PDF that can be stored in any system of record.

- i) Process for retrieving information required to meet eDiscovery requests when documents are stored at a Vendor operated or controlled site; or when information retrieval requires participation of the Vendor or a third party.

Signed agreements can be downloaded any-time from Adobe Sign via the Adobe Sign dashboard, turn-key integrations, or through APIs. By default, signed documents will be stored on Adobe Sign at no cost. To promote compliance with your organization's data retention policies, your account can be configured to delete and purge the signed documents from the service after a specified date or time.

- j) Process for searching and sorting information stored at Agency site to meet eDiscovery requests (e.g. – record identifiers).

Signed agreements can be downloaded any-time from Adobe Sign via the Adobe Sign dashboard, turn-key integrations, or through APIs. By default, signed documents will be stored on Adobe Sign at no cost. To promote compliance with your organization's data retention policies, your account can be configured to delete and purge the signed documents from the service after a specified date or time. Documents can be stored within any system of record for record management (SharePoint, Documentum, etc)

- k) Exit Strategy –Define how this process would work and what costs would be involved. Is there a cost for transferred data?

Adobe Sign allows customers to download signed documents and associated audit reports at any time via Adobe Sign dashboard, turn-key integrations, or via APIs. This means that signed documents can reside in any application of your choosing. If in the unlikely event that you

choose to end your subscription of Adobe Sign, you can download your documents in bulk from Adobe Sign for your records or via the methods described above.

There are no costs associated with data being transferred from the Adobe Document Cloud.

17) Service Level Agreement (SLA) and Reporting

The ideal solution will have a detailed Service Level Agreement (SLA)

- a) Provide a copy of the proposed Service Level Agreement (SLA). Including notation of optional levels of service and Breaches in SLA from a Financial standpoint.

All SLAs and related things will be discussed during contract negotiations.

- *To give an idea, there are sample support team SLAs which are accessible online, but attached in Attachment V.*
- b) What is the standard service availability that the solution commits to provide in a Service Level Agreement (SLA)? Please provide quantitative response in percentage (%) and any other details to describe this service availability commitment.

All SLAs and related things will be discussed during contract negotiations.

However, the system is available 24/7/365. Adobe Sign data centers deliver high availability (5 9's availability: - 90%, 99%, 99.9%, 99.99% and 99.999%) and tolerate system or hardware failures with minimal impact. Current average is 99.987%, with 10 of last 13 months at 100%.

- c) Is the SLA Financially backed?

All SLAs and related things will be discussed during contract negotiations.

- d) With respect to RPO and RTO, please describe how the solution provided allows for an RPO of 24 hours and an RTO of 24-48 hours. Describe the architectural approach, infrastructure and operating environment that are necessary to meet the stated recovery point and time objectives. In addition, tell us if the proposed solution exceeds those metrics.

Adobe Sign strives to achieve the following disaster recovery parameters for its customers:

- Recovery Time Objective (RTO), which relates to potential downtime. The metric refers to the amount of time it could take to recover from a data loss event and how long it takes to return to service. The RTO for Adobe Sign is 8 hours.
- Recovery Point Objective (RPO), which refers to the amount of data that could potentially be lost during disaster recovery. The time frame is determined by the amount of time between data protection events. The RPO for Adobe Sign is 2 hours.

To meet high availability and stated recovery point and time objectives, Adobe maintains equipment in geographically dispersed data centers running in an Active/Passive configuration. All customer data is continuously replicated in real time between the two sites, enabling a failover should the need arise. The data replicated between the primary data center and the disaster recovery site includes all customer documents, agreements and user information. Data replication is managed over a fully encrypted channel between the data centers. All product and infrastructure changes are kept in sync between the primary data center and the disaster recovery site so that any failover is seamless to Adobe customers.

- e) Describe report and metrics generation capabilities. Show examples of how utilization can be tracked by user or groups of users.

The reporting feature in Adobe Sign lets State of NC business users check Adobe Sign account usage. The user can build his/her own reports and gain complete visibility into the document signing process, while seeing how individual groups or users are doing. Moreover, Adobe Sign provides a dashboard to allow users to have up-to-the minute status on documents out for signature and other roles from anywhere either through a web-app or via mobile app.

Adobe Sign also provides a comprehensive set of reporting features, allowing for detailed reports on the overall progress of workgroups. Senders can also track individual agreements through the Adobe Sign portal but can also leverage the reporting capabilities. Users can create new reports or use the out-of-the-box reports. Reports can also be exported to a CSV file to provide the ability to sending reporting data to other systems.

Customizations are also available on the reports generated in Adobe Sign. Users have the option to choose the interval (e.g. this week, this month, date range, etc.) to report on the workflow of their documents (e.g. status changes). Users can also apply additional filters, such as document name, performance goals, and how to graph agreements by (e.g. date, form, signature type, etc.). Additionally, if you have an Enterprise or Global account, you can run a report that will show you the volume of usage in the entire account broken up by user, group or document for any time range.

- *More information and examples may be found in Attachment V.*
- f) The state will require a rolled-up view of all usage broken down by agency quarterly and yearly; therefore, describe how the solution will allow agencies to run their own usage reports.

Customizations are available on the reports generated in Adobe Sign. Users have the option to choose the interval (e.g. this week, this month, this quarter, this year, date range, etc.) to report on the workflow of their documents (e.g. status changes). Users can also apply additional filters, such as document name, performance goals, and how to graph agreements by (e.g. date, form, signature type, etc.). Additionally, if you have an Enterprise or Global account, you can run a report that will show you the volume of usage in the entire account broken up by user, group or document for any time range.

- *More information and examples may be found in Attachment V.*
- g) The total transaction volume can be tracked by month, by Department/Division/Unit, and reported to DIT.

Yes, the total transaction volume can be tracked by month, by Department/Division/Unit.

- *More information can be found by referencing Attachment V.*

18) Software Support and Maintenance Services

The ideal solution will have established support and maintenance. Please explain the following regarding these services:

- a) Describe how the service desk operates; i.e., service hours, escalation of problems, ticket tracking, reporting of metrics on availability, call scripts, repository of solutions, call back time etc.

Adobe will provide Phone support available 24/7 for all the clients under active contract. Adobe maintains a dedicated geographically dispersed team of technical operations engineers utilizing a “follow-the-sun” model where working hours are allocated during regular business hours. This

global team provides 24x7x365 on-call response support to assist the corporate Adobe incident response team with resolving any disruption to the service as quickly as possible.

Adobe provides Platinum Maintenance and Support programs as annual contract and includes unlimited toll-free phone access to support consultants for authorized contacts from your organization. You'll receive priority-level case response times of approximately 1 hour with 24x7x365 mission-critical support.

- b) Describe how the solution will provide availability and uptime metrics for solution.

The system is available 24*7*365. Adobe Sign data centers deliver high availability (5 9's availability: - 90%, 99%, 99.9%, 99.99% and 99.999%) and tolerate system or hardware failures with minimal impact. Current average is 99.987%, with 10 of last 13 months at 100%. Adobe maintains equipment in geographically dispersed data centers. At any given time, only one data center is "live," while a secondary site acts as a warm disaster recovery site in the event the production site goes offline. All customer data is continuously replicated in real time between the two sites, enabling a failover should the need arise. The data replicated between the primary data center and the disaster recovery site includes all customer documents, agreements and user information.

Adobe provides transparent up-time on our Trust Site. Agencies can view this by visiting the URL at <https://status.adobe.com/>. We even support zero-downtime maintenance, if need be.

- c) Describe the solution's development "sandbox" as envisioned for backend integration efforts with legacy environments.

Adobe Sign provides free developer accounts (sandbox/non-production environments) that can be used separately from the production environment—allowing for ongoing testing of systems and employee training.

Please get in touch with your Account Manager for more details regarding hosting of the same.

- d) Describe how the application changes will be able to be previewed in a "sandbox"/non-production environment prior to changes being made in production.

Adobe Sign provides free developer accounts (sandbox/non-production environments) that can be used separately from the production environment—allowing for ongoing testing of systems. Hence, using these sandbox/non-production environments, State of NC can preview the application changes prior to changes made in production environment.

Please get in touch with your Account Manager for more details regarding hosting of the same.

- e) Describe the management and project team assigned to work with North Carolina.

This will be determined upon contract execution. As part of our post-sales on-boarding and customer success management (CSM) process, State of North Carolina will be assigned appropriate resources to ensure the successful implementation of Adobe Sign. Your onboarding specialist will discuss your case goals and objectives, work with you a deployment strategy and introduce you to useful training tools and Adobe learning resources. After your on-boarding specialist helps a department deploy their use case, the CSM will show how to maximize the benefit of your investment. The CSM becomes the trusted advisor for North Carolina and the use of Adobe Sign.

Other resources, such as Adobe Professional Services or third-party integrators can be engaged as needed.

- f) Describe the process for incident management, change management and release management.

In case of a service disruption, Adobe Sign operations team will invoke Adobe's incident management process. When this process is invoked, 24*7*365 on-call engineers are brought together via online collaboration tools in order to triage, solve and resolve the issue. The incident management process also has provisions to capture data on the chain of events leading to the issue. Any outstanding issue is transitioned to the problem management team for ongoing governance.

Adobe enforces a comprehensive, standards-compliant change management process with rigorous inspections to assess potential impacts and benefits for any changes to the Adobe Sign service. Most of the changes have no impact on the services. However, there are rare exceptions, such as an annual disaster recovery procedures test that may impact the customer experience. In such cases, Adobe will provide advance notification to any potentially impacted Adobe Sign customer.

If it is determined that professional services are required, the project will be scoped and a SOW will be created. This would be the only scenario where a change management plan may be needed. In this case, the communication usually occurs via email or verbally. Adobe will document the change request and the professional services team will provide a written schedule change or fee change. This change must be agreed to by both parties before proceeding.

Adobe Sign releases updates with minor cycles getting released quarterly and major release annually. Thus, there are 3-4 minor releases per year and a major release in every 12 months. Updates and new releases are included during the time in which the agreement is in force. All customers are notified before the launch via email and through their Account Manager (CSM) about the upcoming changes. Adobe Sign updates are automatically applied for all customers. For new functionality, customers are notified prior to release and given the option to opt-in to new features.

- g) Provide a list and description of the required roles and level of staff resources to manage, monitor, maintain and support the overall solution.

Adobe is committed to your success with Adobe Sign. The following Adobe stakeholders are here to assist you.

- Account Executive
- Solutions Consultant
- Customer Success Manager / Account Manager
- On-Boarding Team
- Technical Support
- Professional Services

- *More detailed information on our customer support services can be found in Attachment W.*

19) Training

The State desires a solution that will employ training techniques with the capability to accommodate various levels of users. Training will be needed for each department/division/unit to include form modification, workflow creation/modifications, and assistance with onboarding users including signature creation. Describe the solution's training regarding:

- a) What modes of user training are available?

Available training resources include:

- On-demand training videos
- Adobe Sign online help
- Adobe Sign reference guides
- Best practice articles
- 5 steps to developing an effective training plan
- Adobe Sign: Ask Me Anything Webinars
- Quarterly best practice-focused webinars via email invitation

State of NC may absolutely link directly to any of Adobe's support materials.

b) What level of training comes with the proposal?

End-user education, technical training and adoption are key components of every successful deployment. To prepare you for end user training, you'll receive best practice guides like Creating an effective deployment communication plan and 5 steps to developing an effective training plan. To enable a successful launch, the Onboarding Specialist will train your administrative team to effectively manage and scale your account, guiding them in hitting key milestones.

In conjunction with your admins, Adobe offers co-hosting for your first end user training session, which can be recorded and provided as a reusable deliverable. Additional end-user and administrator training, along with custom training videos, is available separately through Adobe Professional Services. Adobe will work with State of NC to develop an appropriate training plan based on your individual business needs and timing. As you begin to extend e-signatures into additional workflows and use cases, your Account Manager will ensure you have the resources, training, and support you need to be successful.

Your Account Manager can also connect you with additional paid services if needed, such as professional services, group training, or extended support.

- *Please see Training Plan on page 14 of the Implementation Guide, found in Attachment X.*

c) What type of training will be provided in the proposal for the new use cases and purchases? (to include form modification, workflow creation/modifications, and assistance with on-boarding users including signature creation.)

Training is available both during the implementation cycle and on an ongoing basis thereafter. Hence, whenever there are new use cases and purchases, State of NC users will get comprehensive training to effectively manage and scale your account.

d) What online help capabilities are available for users?

Adobe Sign includes "ShowMe" help integrated throughout the system providing contextual help across the product.

- *Additional help/documentation files and tutorials are available online, with a preview found in attachment Y.*

e) What online help capabilities are available for administrators?

Adobe Sign includes "ShowMe" help integrated throughout the system providing contextual help across the product.

- *Additional help/documentation files and tutorials are available by viewing the Admin Guide, found in Attachment O.*

f) What web-based documentation is provided?

Web-based documentation files and tutorials are available at:

<https://helpx.adobe.com/support/sign.html>.

- *Please refer to Attachment X and Y for more information.*

g) What live and web-based technical support is provided?

Adobe will provide Phone support available 24/7 for all the clients under active contract. Adobe maintains a dedicated geographically dispersed team of technical operations engineers utilizing a “follow-the-sun” model where working hours are allocated during regular business hours. This global team provides 24x7x363 on-call response support to assist the corporate Adobe incident response team with resolving any disruption to the service as quickly as possible.

h) What types of training and documentation is provided for API usage?

- *For complete API documentation and usage, please reference Attachment N.*

Also, any additional training on APIs is available separately through Adobe Professional Services.

i) Describe the ability to provide cloud based user “sandbox” areas to support user on boarding, training, and functional trials. Specifically discuss limitations as related to function of the production system as well as trial or usage limits.

Adobe Sign provides free developer accounts that can be used separately from the production environment—allowing for ongoing testing of systems and employee training. Generally, there won't be any limitations as such as sandbox environments will have all functionalities same as production environments. Please get in touch with your Account Manager for more details regarding hosting of the same.

Additionally, Adobe currently provides 14 day free trial of Adobe Sign for individuals and organizations and 30 day enterprise trials are available through the enterprise sales team. You can register for the trial at following link by providing necessary details:

<https://acrobat.adobe.com/in/en/sign/free-trial-global.html>

j) Describe whether the proposed solution requires customer to procure or implement any additional, on-premise hardware or technology commodities for proposed solution to function. Specify requirements by including descriptions, manufacturers, and model numbers.

No, State of NC doesn't need to procure or implement any additional, on-premise hardware or technology commodities for proposed solution to function. Adobe Sign is a 100% browser based system and can run on any device with just browser support.

- *Please refer to Attachment Y for a complete listing of the minimum system requirements.*

k) Provide information regarding user communities and/or support groups.

State of NC can access our Adobe Sign services community. Through the community, you can take advantage of blogs and FAQs, submit feature requests, and connect with other Adobe Sign customers to share best practices and lessons learned.

Additionally, Adobe has multiple user conferences annually. Adobe Max and Adobe Summit are annual events that attract a large number of users across multiple Adobe product lines. The most recent Adobe Summit was March 25-29, 2018 in Las Vegas. Information can be found

here: <https://www.adobe.com/about-adobe/pressroom/summit.html>

Local user groups meet more frequently and vary based on product interest.

- *Please refer to Attachment Y for more locations of user communities and support groups.*

Completed Cost Offer

OFFER COSTS: The Vendor must list and describe any applicable offer costs which may include the following:

- 1) Vendor shall be able to accept individual and/or Agency Wide Purchases on behalf of the agency and count toward the tiered pricing of that Agency.

Yes

- 2) Can Transactions/licensing fees be billed by Department/Division/Unit?

Yes

- 3) Pricing based on total transaction volume for the State.

No. Pricing is on the transactions done by each individual department.

- 4) Explain usage and meaning of document, folder, and transaction system identifiers. Usage counts will need to correspond with Cost Proposal in Section IV.

A transaction equals one or more documents executed/sent by a human or a system to one or more recipients. Each recipient may interact with one or more documents in different way based on their roll. The transaction counts whether it is completed, cancelled or deleted.

- 5) Describe the purchase process for an Agency.

The Agency will reach out to their appointed CDW•G representative who will be able to quote and price the opportunity for the Agency by working with Adobe.

- 6) Define the minimum transaction purchase.

Charges start at 100 Transactions.

- 7) Define the Costs for Connectors to *SharePoint, Dynamics 365, Salesforce etc.*

- a) What costs are there to integrate into SharePoint?, Azure, Amazon Webservices, Dynamics 365, and Salesforce.com.

There is no cost for connectors.

- b) What other CRM solutions or cloud solutions do you integrate with? Provide list and a cost for each.

CRM's supported by Adobe Sign are Salesforce and Microsoft dynamics. There is no charge for connectors. If the connector does not already exist, API's can be easily created to integrate with other systems and come with full documentation. In addition, there is no charge for the API.

- 8) Define what is included in the Named users, Tiered, and unlimited pricing models. Support, training, adoption etc.

All aspects of the product are included in each of the models. This includes training, support, and connectors provided by Adobe.

- 9) Define Unlimited or Enterprise in terms of who can utilize this model.

Tiered pricing will include 500,000, 750,000, and 1,000,000 transactions. Cost for transactions start at 100 and we can quote down to 1 named user. If that requirement is met, this model can be utilized.

- 10) Define what constitutes a transaction from a cost standpoint? Specifically, Voided Transactions and bulk Downloads.

A transaction equals one or more documents executed/sent by a human or a system to one or more recipients. Each recipient may interact with one or more documents in different way based on their roll. The transaction counts weather it is completed, canceled, or deleted. Each time a unique document is sent to unique person or set of persons that counts as an individual transaction.

11) Define Adoption accelerator costs if offered?

There are no Adoption Accelerators offered

12) Define the service level, description and costs for Standard, Premium, and Dedicated Support?

All purchase levels will receive the same no-charge support.

13) Is Unlimited phone technical support available for users, power users and administrators?

Unlimited phone technical support is available for all users.

14) Define what happens to the number of Transactions that are not used during the contract term and yearly anniversary.

The unused transactions disappear on a yearly basis with no roll up. If the number of allowed transactions exceeds 1,000,000, there is a true up process.

15) Define the licensing model offered and how signatures and transactions are counted.

This is a tiered system with charges starting at 100 transactions and going up to 1,000,000. A transaction equals one or more documents executed/sent by a human or a system to one or more recipients. Each recipient may interact with one or more documents in different way based on their roll. The transaction counts weather it is completed, canceled, or deleted. Each time a unique document is sent to unique person or set of persons that counts as an individual transaction.

16) NCID Integration-This is a de-centralized model and each Agency will have its own solution; therefore, define the cost for integration. Consider

a) Storage – How much storage is included with each cost model.

Unlimited.

b) Exit Strategy – Define the cost for downloading transactions- Define how this process works

There is no cost. The process for this is defined in the technical section of this RFP.

c) What is the cost for bulk retrieval of documents?

There is no separate cost for retrieval of documents.

d) Migration costs from existing signature systems

Adobe does not charge for migration.

e) Are there costs for Voided Transaction if any?

If a transaction is voided it still counts as a transaction.

f) Is there customization required or proposed addressing specification. If so, what is the cost.

No customization is required.

g) Are there additional modules required or proposed addressing specifications

No, there are no additional modules required or proposed addressing specifications.

h) Are there any installation/conversion/integration/transition costs?

These costs are provided by Adobe at no cost to the Agency.

i) Provide all training costs by type; user, admin, power user. What is included in each cost model.

All is training included through Adobe.

j) Maintenance costs per year- Is this an evergreen product and updates are included?

Maintenance cost is included.

k) Do you have a professional consulting service or other value added service based on hourly rates? Provide your hourly costs. Travel and lodging expenses, if any, must be thoroughly described; and are limited by the State's Terms and Conditions.

Pricing will depend upon engagement.

Item #	QTY	Unit	Description	Ext Cost
1.	1	User/year	Named User	\$567.00
2.	5	Users/year	Named User	\$567.00
3.	25	Users/year	Named User	\$504.00
4.	100	Transaction/year	Package of signatures	\$3.68
5.	500	Transaction/year	Package of signatures	\$3.41
6.	2500	Transaction/year	Package of signatures	\$3.15
7.	5000	Transaction/year	Package of signatures	\$2.63
8.	10000	Transaction/year	Package of signatures	\$2.36
9.	20000	Transaction/year	Package of signatures	\$2.00
10.	50000	Transaction/year	Package of signatures	\$1.42
Item #	QTY	Unit	Description	Ext Cost
11.	75000	Transaction/year	Package of signatures	\$1.26
12.	100000	Transaction/year	Package of signatures	\$1.12
13.	Unlimited	Transaction/year	Package of signatures	N/A* See below for additional pricing
14.	NA	NA	NCID integration	None as per Adobe
15.	Storage	MB	Cost for Form Storage	None as per Adobe

16.		Per Connector	Connector to Dynamics 365	None as Per Adobe
17.		Per Connector	Connector to Salesforce	None as per Adobe
18.		Per Connector	Connector to SharePoint Online	None as per Adobe
19.		Per Connector	Connector to SharePoint On Prem	None as per Adobe
20.			Bulk retrieval of Transactions	Standard cost per transaction
21.		Per hour?	Migration Costs	None as per Adobe
22.	Vendor Define	Transaction/year	Costs for Voided Transactions	Same as standard transaction cost
23.	Vendor Define	Per hour	Professional Services	

Pricing beyond 100000:

500000 transaction/year = \$1.02

750000 transaction/year= \$.89

1000000 transaction/year = \$.84

17) PAYMENT PLAN PROPOSAL:

Vendors should note that multiple State agencies will leverage this contract, subsequently requiring the awarded vendor to invoice and provision each individual agency separately.

If Buying licenses/transactions in the middle of the term then they should be co-termed and prorated to the contract anniversary date.

18) **ALTERNATIVE COST RESPONSE:** Vendors who propose an Alternative cost response must submit a separate document labeled "ALTERNATIVE COST RESPONSE".

CDW•G is not submitting an alternative cost response.

References

PANYNJ-PORT AUTHORITY OF NEW YORK AND NEW JERSEY	
Contact Name	Anthony Pecora IT Personnel
Email	apecora@panynj.gov
Phone	(201) 395-5234

NYC PUBLIC LIBRARY	
Contact Name	Jason Ledakowich IT Personnel
Email	dse@nypl.org
Phone	(212) 621-0209

Case Studies



ADOBE CUSTOMER SHOWCASE



Challenges

- Provide citizens with faster government services
- Reach geographically disperse population
- Improve productivity of government employees

Key products used

Adobe Sign and Adobe Acrobat Pro DC within
Adobe Document Cloud
Adobe Creative Cloud for enterprise
Microsoft SharePoint

Increasing government efficiency in the Aloha state.

State of Hawaii aims to enhance services through paperless initiatives powered by Adobe solutions.

ADOBE CUSTOMER SHOWCASE



RESULTS



LESS TIME to process new hires

64,000+

Signed **APPROVALS** returned in hours, not weeks



Electronic signature **TRANSACTIONS** in the first year



Empowers employees to sign anywhere on **MOBILE** devices

Bringing the aloha spirit

From the clear waters of the Pacific Ocean to the active volcanos on

the Big Island, Hawaii is known for its close ties to nature and its unique culture. With population spread across multiple islands,

ADOBE CUSTOMER SHOWCASE

When elected to office, Governor David Ige promoted the idea of paperless workflows. By reducing the amount of paper that the government uses, Governor Ige recognized that the state could cut costs and positively impact the environment. But just as importantly, adopting digital processes, including supporting electronic documents, helps the government communicate more effectively across islands and deliver citizen services as efficiently as possible.

"Government agencies must be responsive to citizens and held accountable, so our departments have to manage a lot of paper trails and signed document approvals. Electronic signatures are essential for paperless initiatives to succeed," says Todd Nacapuy, Chief Information Officer for the State of Hawaii. "[Adobe Sign](#) in [Adobe Document Cloud](#) offers flexibility to encourage adoption and improve processes inside and outside government."

"Using Adobe Sign as part of our state's eSign Services program, we eliminate much of the time previously spent preparing and routing documents. State personnel can sign with just a few clicks, so we can focus on state business and roll out new services faster."

— Todd Nacapuy, Chief Information Officer, State of Hawaii

Embracing change

ADOBE CUSTOMER SHOWCASE

and workflows, the State of Hawaii prefers to offer scalable, versatile solutions that departments can adapt to their needs. When Hawaii began developing its electronic signature capabilities, which the state eventually branded “eSign Services,” Adobe Sign was considered not only for ease of use to get departments up and running quickly, but also for its strong integration with many third-party solutions already used by teams. Departments can work with Adobe Sign as a standalone solution, or integrate it into Microsoft SharePoint workflows.

"Being able to integrate Adobe Sign within existing SharePoint environments and department workflows gives state employees more options for an integrated solution to send and track documents," adds Nacapuy.

Across the state government, more than 64,000 documents were electronically signed in the first year, and the team expects that number to jump substantially. With continued rollout of the state's eSign Services initiative, powered by Adobe Sign, Nacapuy anticipates that as many as 25,000 government employees will regularly use the solution as a signer, document creator, or both. Over time, the number of users could increase by tens of thousands of employees as more government agencies adopt the service.

Serving citizens across islands

With the state population across seven islands, simply getting documents to the right signer can be difficult. With Adobe Sign, people can sign documents from almost any device—laptop, tablet, or even mobile phone. No special app is needed, nor does the signer need to be logged into a state machine.

Several agencies are already adopting the solution. For instance, the State of Hawaii Department of Health is working toward rolling out an electronic process to manage receiving signed immunization forms for each of the state's 180,000 students in K-12 public schools. Signed forms for every student have to be received and filed annually before a student can start school.

The traditional process of sending immunization forms home with

ADOBE CUSTOMER SHOWCASE

electronically sign forms, the state can make it faster and easier for parents and school administrators alike to comply with processes that help keep students healthy and safe.

The automated electronic processes also support busy government administrators and elected officials who frequently travel to meet with constituents. "Many times, officials who sign documents spend a good part of their days out of the office attending meetings or conferences," says Nacapuy. "With mobile signing, people can get their work done wherever they are while meeting their constituent commitments."

"Adobe Sign in Adobe Document Cloud offers flexibility to encourage adoption and improve processes inside and outside government."

— Todd Nacapuy, Chief Information Officer, State of Hawaii

Empowering employees

Accelerated signing dramatically reduces the time that employees spend on paperwork overall. For instance, newly hired government employees, who once spent 2 hours filling out onboarding paperwork on their first day, can complete online forms at home before ever setting foot in the office. In addition, all employees must sign about 30 documents a year on average, from annual tax documents to updated acceptable use policies—a process that can be greatly streamlined with Adobe Sign.

"The HR department can send documents out for signatures to state

ADOBE CUSTOMER SHOWCASE

hours to just 20 minutes."

The integration between Adobe Sign and SharePoint also promises to simplify previously complex authorization workflows. Leave of Absence forms have to be completed, routed, and signed by several managers if an employee is requesting extended time off. The authorizations can vary based on department, length of leave, and other factors. By integrating Adobe Sign into SharePoint workflows, the state can bring greater oversight and efficiencies to managing these requests.

Better services for everyone

The sooner government agencies can approve proposals and contracts, the faster they can roll out new citizen services. Administrative directives need to be reviewed by as many as two dozen managers, while many expenses need approval from the governor's office.

Previously government offices spent so much time printing documents, routing them to offices, and waiting for signatures that approvals could take two weeks or longer. Now a contract can make its way up the chain of approvals and to the governor's desk in just a few hours. "Using Adobe Sign as part of Hawaii's eSign Services, we eliminate much of the time previously spent preparing and routing documents," says Nacapuy. "State personnel can sign with just a few clicks, so we can focus on state business and roll out new services faster."

Through an Adobe enterprise term license agreement (ETLA) for Adobe Sign and [Adobe Creative Cloud for enterprise](#), the State of Hawaii can effectively deliver essential apps into the hands of staff who need it. Working with the ETLA helps the state realize significant cost-saving compared to purchasing solutions and software in a decentralized fashion. As an added benefit, the IT team gains tools that help deploy software across departments. Time that the IT team previously spent managing and tracking licenses is now refocused to continually refine the quality of citizen services.

"The HR department can

ADOBE CUSTOMER SHOWCASE

*signatures to state
employees, and track the
document status for every
signer."*

— **Todd Nacapuy**, Chief Information Officer, State of
Hawaii

"Compared to the total cost of software and solutions by departments acting separately in the past, the Adobe ETLA is helping us keep the total investment at or below historic figures while adding innovative new features, including electronic signatures, increased accessibility, and enhanced access to creative solutions," says Nacapuy.

Already a staple at most government agencies, [Adobe Acrobat Pro DC](#) is used daily by many employees to convert documents to PDF for more secure, streamlined collaboration and sharing. Acrobat Pro DC has also become instrumental as employees post more documents online in PDF that comply with Section 508 accessibility requirements in the Americans with Disabilities Act (ADA).

Within departments, streamlined access to current versions of Creative Cloud apps, such as Adobe Photoshop CC, InDesign CC, and Dreamweaver CC, enable personal information officers and other communications managers to create high-impact, visually engaging materials, without the aid of costly outside creative agencies. In the end, the government spends less and speeds the delivery of higherquality communications to citizens.

"Adobe solutions offer a solid foundation that allow us to work smarter and solve problems in new ways," says Nacapuy. "Through our strong partnership with Adobe, we're transforming how the government works to provide citizens with faster, more effective services."

State of Hawaii

ADOBE CUSTOMER SHOWCASE

Honolulu, Hawaii

[Visit website >](#)

Solution at a Glance

Adobe Document Cloud

- Adobe Sign
- Adobe Acrobat Pro DC

Adobe Creative Cloud

Creative Cloud for enterprise

Adobe Acrobat Pro
DC

Adobe

Dreamweaver CC

Adobe InDesign CC

Adobe Photoshop
CC

Microsoft SharePoint

[Download a PDF of this story >](#)


[Watch the video >](#)


ADOBE CUSTOMER SHOWCASE

Blogs & Community

Support

Adobe

 Change region ▼

Copyright © 2018 Adobe. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) /  AdChoices

Protecting dispersed, diverse communities.

Tulare County Sheriff's Office processes 5,000 documents across a large region with Adobe Sign.



"Adobe Sign gave us an efficient, accelerated workflow that helped us process 5,000 human resources and other business documents in just over a year."

Lieutenant Chris Galvez, Tulare County Sheriff's Office

SOLUTION

Adobe Sign, an Adobe Document Cloud solution

RESULTS

5,000 Contracts processed in **ONE YEAR**



AUTOMATED paperwork improves communications



ONE MINUTE turnaround for electronic documents



Prevents delays with document **VISIBILITY**



Tulare County Sheriff's Office

Established in 1852

Employees: 1,300 (includes full time, reserves, and volunteers)

Visalia, California

www.tularecounty.ca.gov/sheriff/

CHALLENGES

- Efficiently exchange information across dispersed offices
- Quickly secure multiple signatures on HR documents
- Gain insight into document management and speed turnaround using electronically signed documents

SOLUTION AT A GLANCE

- Adobe Document Cloud
- Adobe Sign

For more information

<https://acrobat.adobe.com/us/en/sign.html>



Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Serving a diverse community

Centrally located in California, Tulare County is home to more than 400,000 people in an area covering 4,863 square miles and large tracts of public lands, including Sequoia National Park. Since 1852, the Tulare County Sheriff's Office has worked with the community to improve the quality of life through professional services and community partnerships.

Serving a diverse community, the Sheriff's Department has 1,300 full-time employees and works with volunteers at 21 locations across the county. The dispersed offices made it difficult to share information and handle routine processes, such as obtaining multiple signatures for approvals on human resources documents. "Adobe Sign gave us an efficient, accelerated workflow that helped us process more than 5,000 human resources and other business contracts in just over a year," says Lieutenant Chris Galvez.

Improving county-wide communications

Before implementing Adobe Sign, an Adobe Document Cloud solution, when the Tulare County Sheriff's Office wanted to share documents back and forth between remote offices and headquarters, it relied on email, fax, or scanning documents, as well as volunteers to courier documents. Manually routing personnel forms, policy authorizations, purchase requisitions, and other paperwork prevented accurate tracking of document status, while delaying contract processing and approvals.

Using Adobe Sign, an employee simply uses the widget to generate the necessary form and sends an email to the required signatory—obtaining signatures in a fraction of the time. "We no longer have to deal with paper forms. A requisitions request needs three signatures and a final copy delivered to the business office," says Galvez. "With Adobe Sign, the forms can be completed by all signatories and the business office can receive a signed, more secure PDF copy all in less than a minute."

Automatic tracking prevents delays that previously plagued the process by providing a document status. If a supervisor is unavailable to sign, the document can be rerouted to another authorized signatory by sending the email and document to that person. "The reporting and automatic reminders in Adobe Sign encourage fast response and accountability," says Galvez.

She adds, "Adobe Sign is now used across departments in the Sheriff's Office for every document requiring a signature." Adobe Sign handles non-standard signature workflows, such as using MegaSign to send policies to all employees, or using the fax-back feature to gain a digital copy of wet signature documents. "Employees can even request forms for themselves using online widgets in the system," says Galvez. "Adobe Sign has eliminated our need to handle physical forms, boosting our efficiency and helping us improve costs and efficiencies county-wide."

Improving health, safety, and welfare.

Franklin County delivers efficient, fiscally responsible services with the help of Adobe Sign.



"Adobe Sign is pivotal for our county's growth and IT strategy because it promotes a mobile workforce and increases efficiencies to help us accomplish more with our current staff."

Sean Crager, CIO, Franklin County

SOLUTION

Adobe Sign, an Adobe Document Cloud solution

RESULTS



REDUCES paper costs and physical storage needs



Supports growth with an efficient **MOBILE** workforce



AUTOMATES workflows for greater efficiency



Provides clear audit trails for greater **COMPLIANCE**



Franklin County

Established in 1784

Employees: 686

Chambersburg, Pennsylvania

www.franklincountypa.gov

CHALLENGES

- Update IT systems for enhanced efficiencies with growing mobile workforce
- Create a paperless environment
- Cost effectively add more services to support a growing county

SOLUTION AT A GLANCE

- Adobe Document Cloud
- Adobe Sign

For more information

<https://acrobat.adobe.com/us/en/sign.html>



Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Meeting needs of a fast-growing population

Located in south central Pennsylvania, Franklin County is the fourth fastest-growing county in the state. To enrich social, economic, and environmental vitality, the county provides health, safety, and general welfare services to meet the needs of residents. The county government is dedicated to providing these services as efficiently and effectively as possible.

Franklin County officials realized that as the county grew, they would need to add more services and do so in a fiscally responsible manner. Officials focused on updating IT systems to streamline processes with a more mobile workforce and a paperless environment. "Adobe Sign was the turning point, providing the key e-signature component of our IT solution," says Franklin County CIO Sean Crager.

Compliance and cost savings

With 57 departments supporting a range of citizen services, Franklin County officials regularly have to sign numerous contracts. Previously, documents were signed in triplicate by multiple employees and vendors before receiving final approval from county officials. As a result, top officials were often buried in paperwork and could spend a lot of time faxing documents that didn't have an audit trail.

By integrating Adobe Sign, an Adobe Document Cloud solution, Franklin County has now moved toward a paperless environment with automated document workflows. Employees submit electronic forms to the county's document management system, Laserfiche, and are prompted to submit contracts for electronic signature through Adobe Sign. By eliminating the need to print out multiple copies, Franklin County reduces paper costs and eliminates physical storage needs, which frees up resources for other county efforts.

"Adobe Sign automatically delivers contracts to all required stakeholders, no matter how many signatures we need," says Ed Yonker, Application Software Specialist at Franklin County. "Adobe Sign gives us a clear audit trail at every step, adding visibility into government processes and helping the county meet compliance regulations."

Automatic reminders encourage timely response by notifying officials about pending contracts. The easy Adobe Sign interface enables people to sign at their desks or on their mobile devices or tablets, without sacrificing secure encryption for official documents. "Adobe Sign is pivotal for our county's growth and IT strategy because it promotes a mobile workforce and increases efficiencies to help us accomplish more with our current staff," says Crager.

Financial Information

The Vendor shall provide evidence of financial stability with its response to this RFP as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

CDW•G has included financial results as reported to the FCC for Fiscal Year ending 2017. Below is an excerpt from our 10K covering the required information.

Report of Independent Registered Public Accounting Firm

To the Stockholders and Board of Directors of CDW Corporation and subsidiaries

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of CDW Corporation and subsidiaries (the Company) as of December 31, 2017 and 2016, the related consolidated statements of operations, comprehensive income, stockholders' equity and cash flows for each of the three years in the period ended December 31, 2017, and the related notes and the financial statement schedule listed in the Index at Item 15 (a) (2) (collectively referred to as the "consolidated financial statements"). In our opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the Company at December 31, 2017 and 2016, and the results of its operations and its cash flows for each of the three years in the period ended December 31, 2017, in conformity with U.S. generally accepted accounting principles.

We also have audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the Company's internal control over financial reporting as of December 31, 2017, based on criteria established in Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 framework), and our report dated February 28, 2018 expressed an unqualified opinion thereon.

Basis for Opinion

These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's financial statements based on our audits. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud. Our audits included performing procedures to assess the risks of material misstatement of the financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that our audits provide a reasonable basis for our opinion.

/s/ Ernst & Young LLP

We have served as the Company's auditor since 2011.

Chicago, Illinois

February 28, 2018

CDW CORPORATION AND SUBSIDIARIES
CONSOLIDATED BALANCE SHEETS
(in millions, except per-share amounts)

	December 31,	
	2017	2016
Assets		
Current assets:		
Cash and cash equivalents	\$ 144.2	\$ 263.7
Accounts receivable, net of allowance for doubtful accounts of \$6.2 and \$5.9, respectively	2,320.5	2,168.6
Merchandise inventory	449.5	452.0
Miscellaneous receivables	336.5	234.9
Prepaid expenses and other	127.4	118.9
Total current assets	3,378.1	3,238.1
Property and equipment, net	161.1	163.7
Goodwill	2,479.6	2,455.0
Other intangible assets, net	897.0	1,055.6
Other assets	40.8	36.0
Total Assets	\$ 6,956.6	\$ 6,948.4
Liabilities and Stockholders' Equity		
Current liabilities:		
Accounts payable-trade	\$ 1,317.7	\$ 1,072.9
Accounts payable-inventory financing	498.0	580.4
Current maturities of long-term debt	25.5	18.5
Deferred revenue	194.0	172.6
Accrued expenses and other current liabilities:		
Compensation	129.5	167.6
Interest	21.6	25.1
Sales taxes	43.8	38.0
Advertising	89.2	55.8
Income taxes	15.1	2.6
Other	180.2	147.2
Total current liabilities	2,514.6	2,280.7
Long-term liabilities:		
Debt	3,210.0	3,215.9
Deferred income taxes	196.3	369.2
Other liabilities	52.8	37.1
Total long-term liabilities	3,459.1	3,622.2
Stockholders' equity:		
Preferred stock, \$0.01 par value, 100.0 shares authorized; no shares issued or outstanding for both periods	—	—
Common stock, \$0.01 par value, 1,000.0 shares authorized; 153.1 and 160.3 shares issued, respectively	1.5	1.6
Less: treasury stock, \$0.01 par value, 0.1 and 0 shares held, respectively	—	—
Outstanding common stock, \$0.01 par value, 153.0 and 160.3 shares outstanding, respectively	1.5	1.6
Paid-in capital	2,911.6	2,857.3
Accumulated deficit	(1,834.3)	(1,673.8)
Accumulated other comprehensive loss	(95.9)	(139.6)
Total stockholders' equity	982.9	1,045.5
Total Liabilities and Stockholders' Equity	\$ 6,956.6	\$ 6,948.4

The accompanying notes are an integral part of the Consolidated Financial Statements.

CDW CORPORATION AND SUBSIDIARIES
CONSOLIDATED STATEMENTS OF OPERATIONS
(in millions, except per-share amounts)

	Years Ended December 31,		
	2017	2016	2015
Net sales	\$ 15,191.5	\$ 13,981.9	\$ 12,988.7
Cost of sales	12,741.6	11,654.7	10,872.9
Gross profit	2,449.9	2,327.2	2,115.8
Selling and administrative expenses	1,410.1	1,345.1	1,226.0
Advertising expense	173.7	162.9	147.8
Income from operations	866.1	819.2	742.0
Interest expense, net	(150.5)	(146.5)	(159.5)
Net loss on extinguishments of long-term debt	(57.4)	(2.1)	(24.3)
Gain on remeasurement of equity investment	—	—	98.1
Other income (expense), net	2.1	1.8	(9.3)
Income before income taxes	660.3	672.4	647.0
Income tax expense	(137.3)	(248.0)	(243.9)
Net income	<u>\$ 523.0</u>	<u>\$ 424.4</u>	<u>\$ 403.1</u>
Net income per common share:			
Basic	\$ 3.37	\$ 2.59	\$ 2.37
Diluted	\$ 3.31	\$ 2.56	\$ 2.35
Weighted-average common shares outstanding:			
Basic	155.4	163.6	170.3
Diluted	158.2	166.0	171.8
Cash dividends declared per common share	\$ 0.6900	\$ 0.4825	\$ 0.3100

The accompanying notes are an integral part of the Consolidated Financial Statements.

CDW CORPORATION AND SUBSIDIARIES
CONSOLIDATED STATEMENTS OF COMPREHENSIVE INCOME
(in millions)

	Years Ended December 31,		
	2017	2016	2015
Net income	\$ 523.0	\$ 424.4	\$ 403.1
Foreign currency translation, net ⁽¹⁾	43.5	(78.5)	(44.5)
Unrealized gain from hedge accounting, net ⁽²⁾	0.2	—	—
Other comprehensive income (loss), net of tax	43.7	(78.5)	(44.5)
Comprehensive income	<u>\$ 566.7</u>	<u>\$ 345.9</u>	<u>\$ 358.6</u>

(1) Net of tax expense of \$0.2 million , \$0.2 million and \$0.3 million , respectively.

(2) Net of tax expense of \$0.1 million for 2017.

The accompanying notes are an integral part of the Consolidated Financial Statements.

CDW CORPORATION AND SUBSIDIARIES
CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY
(in millions)

	Preferred Stock		Common Stock		Treasury Stock		Paid-in Capital	Accumulated Deficit	Accumulated Other Comprehensive Loss	Total Stockholders' Equity
	Shares	Amount	Shares	Amount	Shares	Amount				
Balance as of December 31, 2014	—	\$ —	172.2	\$ 1.7	—	\$ —	\$ 2,711.9	\$ (1,760.5)	\$ (16.6)	\$ 936.5
Equity-based compensation expense	—	—	—	—	—	—	28.3	—	—	28.3
Stock option exercises	—	—	0.1	—	—	—	2.4	—	—	2.4
Common stock issued for equity-based compensation	—	—	0.3	—	—	—	—	—	—	—
Excess tax benefits from equity-based compensation	—	—	—	—	—	—	0.6	—	—	0.6
Coworker Stock Purchase Plan	—	—	0.3	—	—	—	8.7	—	—	8.7
Common stock issued for acquisition of business	—	—	1.6	—	—	—	55.0	—	—	55.0
Dividends paid	—	—	—	—	—	—	—	(52.9)	—	(52.9)
Net income	—	—	—	—	—	—	—	403.1	—	403.1
Repurchases of common stock	—	—	(6.3)	—	—	—	—	(241.3)	—	(241.3)
Foreign currency translation	—	—	—	—	—	—	—	—	(44.5)	(44.5)
Balance as of December 31, 2015	—	\$ —	168.2	\$ 1.7	—	\$ —	\$ 2,806.9	\$ (1,651.6)	\$ (61.1)	\$ 1,095.9
Equity-based compensation expense	—	—	—	—	—	—	33.2	—	—	33.2
Stock option exercises	—	—	0.4	—	—	—	7.4	—	—	7.4
Common stock issued for equity-based compensation	—	—	0.2	—	—	—	—	—	—	—
Coworker Stock Purchase Plan	—	—	0.2	—	—	—	9.3	—	—	9.3
Dividends paid	—	—	—	—	—	—	0.5	(79.2)	—	(78.7)
Net income	—	—	—	—	—	—	—	424.4	—	424.4
Repurchases of common stock	—	—	(8.7)	(0.1)	—	—	—	(367.4)	—	(367.5)
Foreign currency translation	—	—	—	—	—	—	—	—	(78.5)	(78.5)
Balance as of December 31, 2016	—	\$ —	160.3	\$ 1.6	—	\$ —	\$ 2,857.3	\$ (1,673.8)	\$ (139.6)	\$ 1,045.5
Equity-based compensation expense	—	—	—	—	—	—	37.9	—	—	37.9
Stock option exercises	—	—	1.5	—	—	—	13.0	—	—	13.0
Coworker Stock Purchase Plan	—	—	0.2	—	—	—	10.3	—	—	10.3
Dividends paid	—	—	—	—	—	—	0.7	(107.6)	—	(106.9)
Incentive compensation plan shares withheld for taxes	—	—	—	—	0.1	—	(7.6)	(42.0)	—	(49.6)
Net income	—	—	—	—	—	—	—	523.0	—	523.0
Repurchases of common stock	—	—	(8.9)	(0.1)	—	—	—	(533.9)	—	(534.0)
Unrealized gain from hedge accounting	—	—	—	—	—	—	—	—	0.2	0.2
Foreign currency translation	—	—	—	—	—	—	—	—	43.5	43.5
Balance as of December 31, 2017	—	\$ —	153.1	\$ 1.5	0.1	\$ —	\$ 2,911.6	\$ (1,834.3)	\$ (95.9)	\$ 982.9

The accompanying notes are an integral part of the Consolidated Financial Statements.

CDW CORPORATION AND SUBSIDIARIES
CONSOLIDATED STATEMENTS OF CASH FLOWS
(in millions)

	Years Ended December 31,		
	2017	2016	2015
Cash flows from operating activities:			
Net income	\$ 523.0	\$ 424.4	\$ 403.1
Adjustments to reconcile net income to net cash provided by operating activities:			
Depreciation and amortization	260.9	254.5	227.4
Equity-based compensation expense	43.7	39.2	31.2
Deferred income taxes	(172.7)	(97.2)	(54.5)
Amortization of deferred financing costs, debt premium and debt discount, net	5.2	6.5	6.4
Net loss on extinguishments of long-term debt	57.4	2.1	24.3
Loss from equity investments	—	—	11.2
Gain on remeasurement of equity investment	—	—	(98.1)
Mark-to-market (gain) loss on interest rate cap agreements	(0.5)	(2.6)	2.1
Other	0.4	0.4	0.3
Changes in assets and liabilities:			
Accounts receivable	(128.4)	(179.9)	(342.6)
Merchandise inventory	8.5	(68.5)	(31.5)
Other assets	(116.4)	(50.1)	(71.2)
Accounts payable-trade	231.5	225.1	100.5
Other current liabilities	51.4	80.2	47.5
Long-term liabilities	13.7	(30.1)	21.4
Net cash provided by operating activities	777.7	604.0	277.5
Cash flows used in investing activities:			
Capital expenditures	(81.1)	(63.5)	(90.1)
Premium payments on interest rate cap agreements	—	(2.4)	(0.5)
Acquisition of business, net of cash acquired	—	—	(263.8)
Net cash used in investing activities	(81.1)	(65.9)	(354.4)
Cash flows used in financing activities:			
Proceeds from borrowings under revolving credit facility	1,560.7	338.8	314.5
Repayments of borrowings under revolving credit facility	(1,560.7)	(338.8)	(314.5)
Repayments of long-term debt	(14.9)	(20.6)	(32.8)
Proceeds from issuance of long-term debt	2,083.0	1,483.0	525.0
Payments to extinguish long-term debt	(2,121.3)	(1,490.4)	(525.3)
Net change in other long-term obligation	(3.8)	15.7	—
Payments of debt financing costs	(9.6)	(5.9)	(6.8)
Net change in accounts payable-inventory financing	(84.0)	143.6	95.9
Effective portion of interest rate cap agreements	0.4	—	—
Proceeds from stock option exercises	13.0	7.4	2.4
Proceeds from Coworker Stock Purchase Plan	10.3	9.3	8.7
Repurchases of common stock	(534.0)	(367.4)	(241.3)
Payment of incentive compensation plan withholding taxes	(49.6)	—	0.6
Dividends	(106.9)	(78.7)	(52.9)
Principal payments under capital lease obligations	(1.3)	(0.6)	—
Net cash used in financing activities	(818.7)	(304.6)	(226.5)
Effect of exchange rate changes on cash and cash equivalents	2.6	(7.4)	(3.5)
Net (decrease) increase in cash and cash equivalents	(119.5)	226.1	(306.9)
Cash and cash equivalents – beginning of period	263.7	37.6	344.5
Cash and cash equivalents – end of period	\$ 144.2	\$ 263.7	\$ 37.6
Supplementary disclosure of cash flow information:			
Interest paid	\$ (148.5)	\$ (144.3)	\$ (154.6)
Taxes paid, net	\$ (275.7)	\$ (329.2)	\$ (300.2)

The accompanying notes are an integral part of the Consolidated Financial Statements.

Conflict of Interest

- i. Provide a statement that no assistance in preparing the response was received from any current or former employee of the State of North Carolina whose duties relate(d) to this RFP, unless such assistance was provided by the state employee in his or her official public capacity and that neither such employee nor any member of his or her immediate family has any financial interest in the outcome of this RFP;

No assistance in preparing this response was provided by any current or former employee of the State of North Carolina.

- ii. State if the Vendor or any employee of the Vendor is related by blood or marriage to an Agency employee or resides with an Agency employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities within the Vendor's organization of such Vendor employees; and

No CDW employee is related by blood or marriage to an Agency employee or resides with an Agency Employee.

- iii. State the employing State Agency, individual's title at that State Agency, and termination date.

No CDW employee is related by blood or marriage to an Agency employee or resides with an Agency Employee.

Errata and Exceptions

ERRATA OR EXCEPTIONS: Any errata or exceptions must be stated on a separate page, labeled "Errata and/or Exceptions" with references to the corresponding terms or provisions of the Solicitation.

CDW Government LLC accepts the terms and conditions of the RFP and takes no errata or exceptions to this response.

Copy of the Vendor's License and Maintenance Agreements

Vendor Utilization of Workers Outside U.S

VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.: In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer. The Vendor shall provide the following for any offer or actual utilization or contract performance:

- a. The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the Agreement and whether any of this work will be performed outside the United States
- b. The corporate structure and location of corporate employees and activities of the Vendors, its affiliates or any other subcontractors
- c. Notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States
- d. Any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided

Will any work under the Agreement be performed outside the United States?

Where will Services be performed:

YES _____ NO X

Reseller Documentation

Reference to Section V.20

RESELLERS: If the Offer is made by a Reseller that purchased the offered items for resale or license to the Agency, or offered based upon an agreement between the Offeror and a third party, and that the proprietary and intellectual property rights associated with the items are owned by parties other than the Reseller ("Third Parties"). The Agency further acknowledges that except for the payment to the Reseller for the Third Party items, all of its rights and obligations with respect thereto flow from and to the Third Parties. The Reseller shall provide the Agency with copies of all documentation and warranties for the Third Party items which are provided to the Reseller. The Reseller shall assign all applicable third party warranties for Deliverables to the Agency. The State reserves all rights to utilize existing agreements with such Third Parties or to negotiate agreements with such Third Parties as the State deems necessary or proper to achieve the intent of this RFP.

Adobe Phone Support Line: 1 (866) 318-4100

For technical support, the final user can call also CDW Technical Support at 800-383-4239. The agent will verify product and problem and will then transfer the customer to an experienced technician or set up for callback when a technician becomes available. The technician will verify the case notes and will troubleshoot the problem.

If the issue is resolved, the customer receives the case number and the call ends. If the issue requires follow up, the technician will contact the customer at a specified time. If the issue does not require follow up, then the technician will close the case.

If an issue is not resolved it will be escalated to the OEM's technical support. If the issue has been resolved the technician will close the case.

When warranty support is needed, the technician will guide the customer in the direction best suited to resolve the issue.

Adobe Enterprise Term License Agreement

All use of the Licensed Products (including On-demand Services, Managed Services and On-premise Software) specified above (and applicable License Metrics) shall be governed by the applicable Adobe Enterprise Licensing Terms which consist of the General Terms (2017v1) and the applicable Product Specific Licensing Terms ("PSLT"s) which are available at www.adobe.com/legal/terms/enterprise-licensing.html (collectively "Licensing Terms"). Support terms ("Support Terms") can be found on Adobe's website at

http://www.adobe.com/support/programs/policies/terms_customer.html.

Product descriptions (and applicable License Metrics) for the Licensed Products are published by Adobe on <https://helpx.adobe.com/productdescriptions.html>.



PSLT - Adobe Electronic Signature Service (2017v1)

1. **Content Files.** Customer may use, display, modify, reproduce, and distribute any of the Adobe-provided sample files such as fonts, stock images, sounds or templates ("Content Files"), but Customer must not distribute Content Files on a stand-alone basis, or claim any trademark rights in the Content Files, or derivative works of, the Content Files.
2. **Modification.** Adobe may modify or discontinue the On-demand Services or any portions or service features at any time without liability to Customer or anyone else. However, Adobe will make reasonable effort to notify Customer before Adobe makes such changes. If Adobe discontinues an On-demand Service in its entirety, then Adobe will provide Customer with a pro rata refund for any unused fees for that On-demand Service.
3. **Third-Party Software Notices.** The creators or third party licensors of certain public standards and publicly available code ("Third Party Materials"), require that certain notices be passed through to the end users of the On-demand Service. These third party notices are located at <http://www.adobe.com/go/thirdparty> (or a successor website thereto). The On-demand Service, as delivered to Customer, complies with these notices, and the inclusion of these third party notices does not limit Adobe's obligations to the Customer for Third Party Materials integrated into the On-demand Service.
4. **Storage and Retention.** Adobe will store Customer Content and Customer Data during the License Term up to any storage limit specified in the applicable Sales Order. Adobe may create reasonable storage limits, such as limits on file size, storage space, and other technical limits. If Customer exceeds those limits, Adobe will make reasonable efforts to notify Customer to permit transition of Customer Content and Customer Data prior to deletion.
5. **Privacy, Information Security, and Compliance.**
 - 5.1 **Configurable Controls.** Adobe makes certain security controls available and configurable by Customer, or Adobe's customer support. It is Customer's responsibility to determine what notices, consents, and controls Customer requires in order to comply with laws, standards, regulations, or obligations that Customer may have to Customer's Participants. Once Customer sends an Electronic Document for signature, or transfers an Electronic Document out of the electronic signature service, or to a third-party provider, that Electronic Document leaves Adobe's servers, and Adobe's security controls no longer apply. Information received by Adobe in connection with the electronic signature service is governed by the Adobe Privacy Policy (adobe.com/privacy/policy.html), including the Adobe electronic signature services privacy terms (adobe.com/privacy/echosign.html, or successor websites).
 - 5.2 **Security.** Adobe has implemented information security practices to help protect Customer Content. For more information, please see: <http://www.adobe.com/security.html>. However, Customer may not use the fax option in Adobe Sign to process payment card information, including credit card numbers and verification codes.
 - 5.3 **Sensitive Personal Information.** The Sensitive Personal Data section of the General Terms does not apply to Customer's use of the electronic signature service.
6. **Legal Counsel.** Customer will rely on its own legal counsel and determinations as to the use and viability of electronic signatures in a particular country or for a particular use.
7. **Digital Certificates.** Digital certificates are generally provided by third parties and not Adobe. Customer is responsible for deciding whether to rely on a digital certificate, and Customer's use of digital certificates is at Customer's sole risk.

8. Additional License Restrictions. Customer must not: (A) place advertisement of any products or services through the On-demand Services; or (B) impersonate any person or entity, or falsely state or otherwise misrepresent Customer's affiliation with a person or entity.

9. Additional Definitions.

- 9.1 **"Electronic Document"** means any document uploaded into the electronic signature service.
- 9.2 **"Participant"** means an individual or entity that electronically reviews, accepts, signs, approves, transmits, or delegates action to a third party regarding Electronic Documents via Customer's electronic signature service account.
- 9.3 A **"Transaction"** occurs each time an Electronic Document, or collection of related Electronic Documents up to 100 pages or 10 MB are sent to Participants through the On-demand Services.

Support Services | Terms and conditions



The following provisions detail Adobe's provision of support services to an eligible entity ("Customer") for the applicable On-premise Software, On-demand Services, and Managed Services (collectively, the "Products"). These support services (or portions thereof) ("Support Services") may have been previously referred to as Gold, Platinum, or Enterprise Support Services. More information regarding eligibility and applicability of these Support Services may be obtained by contacting Adobe Customer Care.

✓ Live Telephone and Online Technical Support

Adobe will provide live technical support services to up to ten (10) individuals designated by Customer on a 24x7x365 basis. Local language support, if offered, is available from 9:00 am through 5:00 pm Monday through Friday local time, excluding national holidays and Adobe designated holidays. Outside these hours, support is available in English language only. Upon enrollment, Adobe will provide Customer with appropriate telephone numbers to be used for support, and the support sites to be accessed for unlimited online support, depending on the geographical location of Customer and Adobe Products licensed.

✓ Remote Support

Customer may request support services via remote computer access. If so requested, Customer agrees to allow Adobe permission to remotely access any and all Customer systems on which the Adobe Products depend, via an external computer controlled by Adobe, for the sole purpose of providing support services to Customer.

✓ Expert Services Appointments

If available for a Product, Customer's designated technical support contacts may schedule expert services appointments consisting of up to 30 minutes of telephone advice regarding product workflows and best practices. Customer may contact Adobe Customer Care to inquire if such appointments are available for a specific Product.

✓ Initiation and Processing of Service Request

To initiate a request for support services from Adobe, Customer's designated individual must identify the failure of the applicable Product to perform in accordance with the applicable published product documentation ("Service Request"). After receipt of a Service Request, Adobe will (a) define the priority of the Service Request, and (b) undertake reasonable efforts to acknowledge receipt of such Service Request within the identified timeframe ("Targeted Response Time") via the same medium of communication by which the Service Request was reported.

The priority of each Service Request will addressed as follows:

Priority	Description	Targeted Response Time
Level 1 - Critical	Problem results in extremely serious interruptions to a production system Tasks that should be executed immediately cannot be executed	30 minutes (Service Request must be initiated telephonically)

	<p>due to complete crash of a production system or interruptions in mainfunctions of a production system</p> <p>Problem results in compromised data integrity which could result in financial losses</p> <p>Problem has affected or could affect entire user community</p>	
Level 2 - Urgent	<p>Problem results in serious interruptions to normal operations and could negatively impact an enterprise-wide installation or urgent deadlines in a production system</p> <p>Data processing continues but in a restricted manner and data integrity may be at risk which may cause serious interruptions to critical processes</p> <p>Problem hinders the deployment of an enterprise installation of a pre-production system</p>	1 hour

Level 3 - Important	<p>Problem causes interruptions in normal operations or minor degradation in performance</p> <p>Problem is attributed to malfunctioning or incorrect behavior of the Product</p>	4 hours
Level 4 - Minor	<p>Problem results in minimal or no interruptions to normal operations but no business impact</p> <p>Problem typically consists of installation and configuration inquiries</p>	1 business day

✓ Processing of Service Request

Adobe will use reasonable efforts to acknowledge receipt of the Service Request within the Targeted Response Time. Adobe will use commercially reasonable efforts to diagnose the problem and provide a remedy that could take the form of eliminating the defect, providing updates, or demonstrating how to avoid the effects of the defect using a commercially reasonable level of effort. Despite Adobe's exercise of reasonable efforts, not all problems may be solvable. The processing time will start from the date and time when Adobe's Customer Care team acknowledges receipt of the Service Request. If the Service Request cannot be solved within a commercially reasonable timeframe, the Service Request may be escalated within the Adobe

Customer Care organization. Customer's designated technical contact must be available to work with Adobe Customer Care while Adobe is in the process of resolving the Service Request.

✓ **Right to Modify Targeted Response Times**

Adobe reserves the right to alter the Targeted Response Times, from time to time, using reasonable discretion but in no event may such alterations result in: (a) diminished support from the level of support described herein; (b) materially diminished obligations for Adobe; or (c) materially diminished rights of Customer. Adobe will provide Customer with 60 days prior written notice of any material changes to the Targeted Response Times identified herein.

✓ **Issuance of Updates**

In its sole discretion, Adobe may provide Customer with an update to a Product which may consist of code corrections, bug fixes, and minor modifications or enhancements to the Product in order to bring the Product into substantial conformity with the applicable published product documentation. Updates will only be provided to Customer for the current version of the Product. All updates are provided to Customer on a license-exchange basis. Adobe's issuance of an update to a Product is intended as a replacement of the copy of the Product previously licensed to Customer and are not provided as additional copies.

✓ **Maintenance: Issuance of Upgrades**

The following provision applies to: purchases of On-premise term licenses, On-demand Services, and Managed Services and purchases of On-premise perpetual licenses, only if Customer is enrolled in a maintenance and support

program. As used herein, "Upgrades" means an upgrade to a Product consisting of a new version release of the Product, or a generally available modification or enhancement to the performance or functionality of the Product that exists in the then-current release of such Product. In its sole discretion, Adobe may provide Customer with an Upgrade to a Product. All Upgrades are provided to Customer on a license-exchange basis. Adobe's issuance of such Upgrade to a Product is intended as a replacement of the copies of the Product previously licensed to Customer and are not provided as additional copies. Copies of the Products that are replaced must be destroyed. Customer's use of any Upgrade provided by Adobe is to be governed by the updated license use and restriction terms in the applicable end-user license agreement, if any.

✓ **Right to Discontinue or Modify Support**

Adobe has the right to alter, or discontinue the manufacture and development of any of the Products and the support available for those Products, at any time in its sole discretion, provided that Adobe agrees not to discontinue the support for a Product during Customer's then-current, paid for, support term, subject to the termination provisions in the applicable end-user license agreement between Customer and Adobe, or these terms and conditions. In no event will such alterations made to support during Customer's then-current support term result in: (a) diminished support from the level of support set forth herein; (b) materially diminished obligations for Adobe; or (c) materially diminished rights of Customer. Adobe will provide Customer with sixty (60) days prior written notice of any material changes to the support services contemplated herein.

✓ **Additional terms applicable to perpetual On-premise**

Software licenses

Renewal Fees

If Adobe makes renewals for support available to its customers generally, Adobe will provide Customer with a renewal notice in advance of expiration of the then-current term for support services, so that Customer can order an additional one year term for support. If Customer desires to renew, Adobe will invoice Customer for the renewal term. If Customer allows its support services on its perpetual license to the On-premise Software to lapse, Customer may be subject to additional fees, to cover the lapsed period, prior to the reinstatement of support services. If Customer elects to renew support services for an additional term following the purchase of the On-premise license, the renewal annual support fee is determined as follows: (a) for the first renewal term, the initial annual fee may be increased by three percent (3%); (b) for the second through the fourth renewal terms, the annual support fee for the immediately preceding renewal term may be increased by three percent (3%); and (c) for the fifth and subsequent renewal terms, the annual support fee will be the lesser of twenty percent (20%) of the then-current list price for the On-premise Software or the annual support fee for the immediately preceding renewal term increased by the applicable Consumer Price Index (CPI), for the twelve-month period preceding the renewal date, however, in no event shall the amount be less than the annual support fee charged for the prior year for the On-premise Software covered by the applicable renewal.

Decommissioning

If Customer has purchased multiple perpetual licenses of an On-premise Software and Customer chooses to renew

support services, Customer must purchase support services on all of the perpetual licenses of the On-premise Software unless otherwise agreed by Adobe and which would be subject to Adobe's policies on documenting decommissioned On-premise Software licenses.

Extended Support

If the version of an On-premise Software product licensed by Customer reaches end of life, Customer may elect to purchase extended support ("Extended Support") for a maximum period of another two (2) years from the end of life date, provided that Extended Support is available for that version of the On-premise Software. The [Support Lifecycle Policy](#) identifies the availability of Extended Support and its associated cost.

Resources

[Support services for purchases prior to 23 May 2016](#)



Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)

[^ Back to top](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region 

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [AdChoices](#)

CDW's Letter of Authorization for Adobe



Adobe Systems, Incorporated

345 Park Avenue
San Jose, CA 95110-2704
Phone 408 536.6000

August 17, 2017

To Whom It May Concern:

This letter confirms the participation of CDW Corporation, in the Adobe North American License Center (ALC) Program, which includes authorization for Adobe's Value Incentive Plan (VIP) and Cumulative Licensing Program (CLP) in all customer segments: Commercial, Education, Government, Government-GSA, Non-Profit, and Adobe Enterprise Agreement 2 (EA2) for Commercial and Government segments, and FLP License Programs for all Adobe Desktop Software Products and Adobe LiveCycle Products. This authorized product list includes desktop products from the former company Macromedia, Inc.

CDW Corporation continues to perform to Adobe's highest level of satisfaction under the program guidelines and parameters, and remains Adobe's Number One ALC License Program Partner.

CDW Corporation is an authorized reseller for shrink-wrap product in the Commercial, Government, and Education markets. They are also authorized in these markets to resell our Transactional Licensing Program (TLP) and our Forms License Program (FLP), which includes Captivate and Connect.

Adobe's VIP, CLP, and EA2 Government, and CLP, EA2, VIP and FLP Commercial program licenses are purchased direct from Adobe by our authorized ALC's. Adobe shrink-wrap (all segments), TLP licenses (all segments), VIP and CLP Education, and FLP Government licenses are purchased from Adobe's authorized Distributor Channel.

If a Vendor responds to the **Adobe Education** portion of an RFQ or RFO, Adobe Systems, Inc. must confirm the Vendor's Adobe Education Reseller authorization.

If a Vendor responds to the **Adobe Government** portion of an RFQ or RFO, Adobe Systems Inc. must confirm the Vendor's Adobe Licensing Center (ALC) authorization for Government or Government GSA.

Please direct any further inquiries to Matt VanderZee, Senior Channel Sales Manager, Adobe Systems Incorporated.

Thank you,

Matt VanderZee

Matt VanderZee
Senior Channel Sales Manager
Adobe, North America Channels
PH: 773-206-4579
vanderze@adobe.com

North Carolina Business License

Issued by the Secretary of Revenue

Merchant's Certificate of Registration

CDW GOVERNMENT, INC.
230 N MILWAUKEE AVE
VERNON HILLS IL 60061



Date Issued: April 11, 2002
County: FOREIGN
Business Class: 5180
City Code: 0101000
County Code: 101
License No: 000744145

Other Supporting Materials Including Technical System Documentation

Attachment F- Incident Response Overview (pg 109)

Attachment AA- Adobe Sign Migration Services (pg 115)

Attachment AB- Adobe Sign for Microsoft Office 365 (pg 117)

Attachment D- Certifications, ISO, FedRAMP (pg 119)

Attachment E- Agreement Encryption Methods (pg 124)

Attachment G- Transform Business Processes with Electronic and Digital Signatures (pg 128)

Attachment H- Audit Trail (pg 139)

Attachment I- Compliance Overview (pg 143)

Attachment J- Adobe Sign Technical Overview (pg 148)

Attachment K- Archiving Agreements Externally (pg 159)

Attachment L- Multilanguage Sending and Signing (pg 170)

Attachment M- Business Partners, Integration Solutions (pg 174)

Attachment N- API Documentation (pg189)

Attachment P- Adobe Sign for Microsoft (pg 191)

Attachment Q- Adobe Sign Voluntary Product Accessibility Template (pg 227)

Attachment R- Form Field Validations (pg 238)

Attachment S- Adobe Sign Workflow Designer (pg 243)

Attachment T- Agreement Field Types (pg 254)

Attachment U-Set Reminders (pg 260)

Attachment V- Adobe Support Policies: Service Level Agreements (pg 265)

Attachment W- Adobe Onboarding Program, Adobe Professional Services, Extended Service Offering (pg 278)

Attachment Z- Solution Brief (pg 286)

Incident Response Overview

Overview

At Adobe, the security, privacy and availability of our customers' data is a priority. We believe that a company-wide, cohesive incident response program is as critical to the success of an organization as the company's product strategy. To that end, Adobe implements a comprehensive incident response program that includes proactive security monitoring, reactive incident response to software, service, and industry security incidents, and proactive guidance to ensure that employees across the company benefit from the knowledge learned from incidents. Focused on the greatest areas of risk, our corporate incident response program is designed to help enable our customers' trust in security with Adobe.

Table of Contents

- 1 Overview
- 1 The Adobe Incident Response Organization
- 2 The Adobe Product Incident Response Team (PSIRT)
- 2 Proactive Security Efforts
- 3 Reactive Security Efforts
- 4 Incident Severity Levels
- 6 How Incident Response Impacts Regulatory Compliance
- 6 Conclusion

The Adobe Incident Response Organization

The Adobe Incident Response Organization consists of two (2) main groups:

- **The Adobe Security Coordination Center (SCC)**, which is responsible for all proactive security monitoring and reactive incident response for all Adobe assets across the entire corporation; and
- **The Adobe Product Security Incident Response Team (PSIRT)** drives Adobe's vulnerability disclosure program. By providing customers, partners, pen-testers and security researchers with a single point of contact and a consistent process to report security vulnerabilities identified in Adobe products and services, PSIRT encourages the external security community to disclose security issues privately and in a manner that minimizes risk to customers, Adobe infrastructure and the brand.

The SCC is a centralized group within Adobe that consists of the Adobe Security Operations Center (SOC), which handles monitoring and alerting, a threat intelligence team, and an incident response (IR) team. These teams work together and with other stakeholders within and outside of Adobe to drive the prevention and early detection of security incidents as well as to continuously improve the company's security posture and maturity. The threat intelligence team focuses on threat actors and methodologies, while the SOC team handles alerts and the triage thereof. Once an alert hits specific incident triggers, the incident response team takes over investigation and mitigation of the incident. The SCC also curates and shares vetted security intelligence to appropriate groups across the organization, to ensure that employees within Adobe benefit from the knowledge learned from incidents.



Figure 1: The Adobe Security Coordination Center (SCC) works with internal and external stakeholders to continuously improve the company's security posture and maturity.

The Adobe Product Incident Response Team (PSIRT)

While the SCC handles general threats to Adobe cloud services, infrastructure, and proprietary corporate information, Adobe PSIRT manages the response to Adobe product vulnerabilities disclosed or discovered by third parties, specifically those that come from independent security researchers. PSIRT encourages private disclosure in a manner that minimizes risk to customers, Adobe infrastructure and the Adobe brand. Adobe PSIRT provides a communication channel for industry partners, independent researchers, CERTs and other stakeholders to privately disclose security vulnerabilities impacting Adobe software, services and infrastructure. PSIRT validates these submissions, and then works with the impacted technology owner to remediate or mitigate the vulnerability.

Proactive Security Efforts

Adobe's proactive security issue identification efforts include continuous monitoring of Adobe services and infrastructure as well as industry threat intelligence information.

Monitoring and Forensics

The security operations center in the SCC uses commercially available security information and event management (SIEM) solutions to consume and analyze various data sources. Local and remote analysis is conducted in a state-of-the-art forensics lab. The SCC uses the information gathered through SIEM to detect potential threats and make intelligent, informed decisions regarding an appropriate response for each threat, whether it is a low-risk, commodity threat or an advanced, high-risk security threat. Employees continually tune the SIEM tool to filter out noise, eliminate false positives, and help ensure the most critical threats are properly prioritized.

Threat Intelligence

Adobe subscribes to industry threat feeds and email lists, which provide threat intelligence information from industry peers as well as adjacent industries. Information is received in a structured format that enables easy distribution into our SIEM systems. Adobe has a multi-faceted threat intelligence program using a combination of automation using industry standard tools and employee reviewers to filter through the intelligence we receive. The combination of external and internal sources is used to appropriately rank intelligence based upon necessary course of action.

Industry Collaboration and Knowledge Sharing

Adobe collaborates with other software vendors and technology companies to share knowledge and security threat information. In addition, Adobe participates in industry organizations, such as [FIRST.ORG](#), [MAPP](#) (Microsoft Active Protections Program) [CISO Coalition](#), [SAFECode](#) (the Software Assurance Forum for Excellence in Code), and [MAAWG](#) (Messaging, Malware and Mobile Anti-Abuse Working Group), as well as other private, inter-company incident response working groups.

Penetration Testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and help improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan.

Reactive Security Efforts

The primary objective of Adobe's incident response efforts is to return systems to a known good state that is free of compromise. Because each security incident is unique, defining rigid, step-by-step instructions for handling each incident is impractical. Instead, Adobe has created a well-defined, methodical flow for each defined security incident.

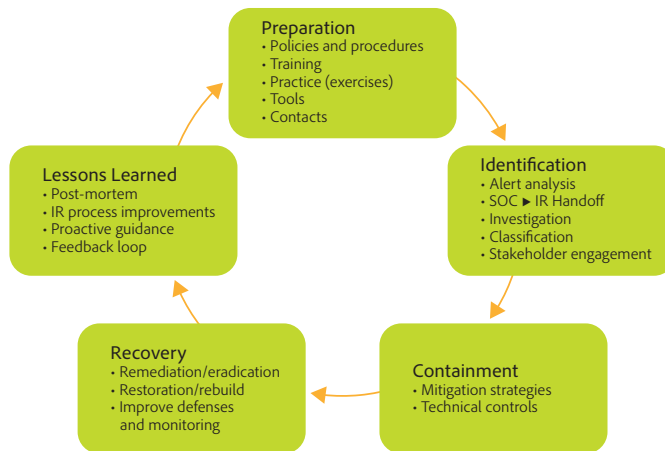


Figure 2: Adobe Incident Response Lifecycle

Phase I: Planning and Preparation

While it is always easier to plan and prepare for security incidents than to repair and recover from them, incidents do occur, despite best efforts and intentions of company employees. In order to help mitigate any potential issues that inhibit the incident response process, Adobe has implemented the following key elements across the company:

- Security policies and procedures
- Alert and Incident response handling methodologies
- Call tree and notification processes for solutions, products and support teams
- Regular skill development, improvement and training for information security staff
- Incident response plan testing, team drills and tabletops
- Collection of threat and vulnerability intelligence
- Tool kit inventory, improvements and regular updates

Phase II: Identification Feedback Loop

Adobe defines a security alert as "a notification or event, that, when taken in conjunction with additional information beyond the event itself suggests a potential threat to a system, environment, process or workflow that may result in disruption of service, liability, brand impact or possible compromise to the confidentiality, integrity or availability of Adobe infrastructure." Security alerts may be system-generated or initiated by an individual, and can take the form of user/customer notification, an anomaly detected by internal Adobe personnel, an alert from a software tool monitoring the network or its endpoints or a communication from threat intelligence channels and security researchers, including crowd-sourced penetration testing organizations.

To be classified as a security *incident*, an alert must be accompanied by confirmation, validation or a reasonable suspicion that an Adobe-defined incident trigger has also been met. The SCC has several defined triggers, including:

- Involvement or compromise of Personal Information (PI)
- Notification about a suspected security incident from an external (non-Adobe) party
- Any security event that impacts the broader technology industry (i.e., issue with commonly used open source code)
- Impact to confidential and/or restricted data
- Suspected malicious access to non-public data
- In-progress active exploitation
- Active or required involvement from law enforcement, legal, customer communications, PR or other third party
- Requested classification of an alert as an incident by any member of the SCC

Any security alert can be escalated to incident status for further investigation when the results of a preliminary investigation are inconclusive.

Incident Severity Levels

Adobe defines incident severity as follows:

Severity	Description	Definition
0	Crisis/Critical	Incident of such severity as to require all available resources and the participation of C-level executives.
1	High	Causing severe impact/damage/disruption to customers, employees, infrastructure. Probable or known impact of restricted data (as defined in the Adobe Data Handling and Classification Standard). Probable or known impact of confidential data (as defined in the Adobe Data Handling and Classification Standard) that is a customer asset or employee, customer, or vendor personal data.
2	Medium	Causing moderate impact/damage/disruption to customers, employees, infrastructure. Probable or known impact of confidential data (as defined in the Adobe Data Handling and Classification Standard) that is not a customer asset or personal data. Known by a third party.
3	Low	Causing minor/negligible impact/damage/disruption to customers, employees, infrastructure. Probable or known impact to internal data (as defined in the Adobe Data Handling and Classification Standard).
4	Informational	Causing no impact/damage/disruption to customers, employees, infrastructure. No action required, but should be tracked.

Figure 5: Adobe incident severity classifications

After a severity level has been set, the SCC begins incident handling and response, which includes gathering data (e.g., logs and forensic images) to help determine the root cause of the incident as well as the best course of action for mitigation.

Phase III: Containment Feedback Loop

The purpose of the containment phase is to limit any damage and prevent any further damage from occurring. Incident handlers work with incident responders within the SCC to understand and document the necessary steps to minimize the effects of the Incident. Based on recommendations from the incident handler, incident responder(s), and other stakeholders, a containment strategy is implemented by the appropriate parties. In the incident containment phase, the SCC considers the following:

- How was the threat launched and from where?
- What assets have been impacted and what damage has been done?
- Is the incident limited to a single machine or has there been lateral movement in the network?
- Do we need to review logs or conduct memory forensics to better understand the threat?
- What is the motive and methodology behind the malicious activity?
- Do we need to gather additional intelligence in order to monitor the threat in other areas of the business?
- What is the service impact upon containment?
- How can we measure and track the success of containment?

Phase IV: Remediation and Recovery

Once the SCC contains a security incident, it moves on to the remediation and recovery phase of the incident lifecycle, which works towards ensuring that systems are cleansed of any malicious or other illicit content and ready to be used again within the organization. The incident handler works closely with stakeholders to determine the timing of incident remediation, eradication and recovery and the assignment of testing and validation. This process may not be swift, as it takes time, careful planning and adequate resources to be successful. While the exact steps involved in remediation and recovery are dependent on the organization and the incident type, the following areas and actions are considered:

- Patching and hardening system images
- Reimaging systems
- Implementing password changes
- Improving monitoring and defenses

Where necessary, customer notification is also covered in this phase of Adobe's incident response lifecycle. If the incident is determined to manifest itself as a product vulnerability, Adobe follows the PSIRT notification process, which includes issuing a customer bulletin about the incident and an estimated timeframe for resolution. Adobe issues another PSIRT bulletin upon implementation of the product fix.

For all other incidents (i.e., non-product vulnerabilities), Adobe immediately issues a customer notification if we are legally or contractually required to do so. Customer notification requirements are governed by the laws and regulations of the countries in which the incident occurred.

Phase V: Lessons Learned

After an incident has been resolved, the SCC enters the final phase of the incident response lifecycle, which includes processes and feedback loops, such as a post-mortem analysis. By conducting a post-mortem analysis for incidents, which highlights what went right and what went wrong, how to better defend the organization, and where the organization should focus resources, the SCC can provide proactive guidance to and drive improvements across the entire Adobe organization and, when required, to supporting processes.

How Incident Response Impacts Regulatory Compliance

A solid, well-thought-out incident response plan is a critical component of regulatory compliance, as most regulations include a formal, documented IR plan as a requirement for compliance. Adobe's robust strategy, outlined in this paper, for both proactive and reactive security measures plays an important role in maintaining compliance. It includes multiple layers of controls to help ensure the security and privacy of customer information as well as Adobe products, creating a fall-back plan if any single control happens to fail. Constant updates to the IR plan help Adobe make sure we stay up to date on the latest incidents and can remain compliant now and in the future.

For information about the various compliance standards and regulations supported by Adobe offerings, please see the [Adobe Cloud Services Compliance Overview](#).

Conclusion

Adobe strives to ensure that our incident response, mitigation, and resolution process is nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help ensure the highest levels of security for all Adobe products and services.

Please visit the Adobe security information site at <http://www.adobe.com/security> for more information about security efforts across our products and services.





Adobe Sign Migration Services.

Adobe has been at the forefront of digital transformation since inventing PDF more than 20 years ago. As the global leader in secure digital documents, we have taken care to design comprehensive migration services to help bring the benefits of Adobe Sign to your organization quickly and efficiently.

Our migration services are based on our experience moving customers to [Adobe Sign](#) from other e-signature solutions. Up to 20 hours of professional services are included free of charge with each service engagement. These complimentary hours are designed to address critical areas to ensure a seamless transition of your e-signature processes.

Service engagements kick off with a stakeholder meeting designed to understand the project's needs and challenges. Working with subject matter experts from your organization, the project's objectives, goals and priorities are defined. Adobe solution architects then develop a comprehensive description of the requirements to inform a statement of work (SOW) that specifies the process and tasks to be executed, along with the estimated hours.

Adobe Sign expert and trusted migration services include both automated services and solution architect guided tasks. Because every customer is unique, the complimentary service hours can be applied flexibly towards any of these services.

Should a customer require additional services to supplement the migration services, professional service hours can be purchased at the standard rate of US \$250/hour. All customer engagements will be provided with onboarding, Customer Success Manager (CSM), and support resources per any standard enterprise purchase.

Our experienced Professional Services team partners with your organization to ensure your move to Adobe Sign is organized and efficient, enabling you to quickly realize the full value of Adobe Sign.

Automated migration services.

Our solution architect team has developed a number of trusted tools to automate key migration functions. The service hours include use of these tools and consulting time to ensure that tasks are completed successfully.

User migration.

A key part of any migration is ensuring that all users who were able to use the previous system can use Adobe Sign. The user migration is an automated process that utilizes APIs to retrieve user information. Once it is extracted, the tool then leverages the Adobe Sign API to create matching user accounts in Adobe Sign.

Document export tool and training.

Ensuring the safe retrieval and storage of all documents from a previous solution is a baseline requirement for the success of an Adobe Sign implementation. The document export tool automates the retrieval of all previous documents. Using APIs, the tool is designed to be run by the customer to initiate the secure download of all documents from the previous system. Your team members will be trained and will have unlimited use of this automated tool.

Template conversion.

Many customers have e-signature document templates to speed and systematize the use of frequently used forms. The migration services include a template conversion tool to convert downloaded templates into Adobe Sign compatible, tagged PDFs.

Solutions team guided tasks.

As the SOW is being defined with the customer, the following integrations and the business workflows related to them are evaluated. Once the use cases are clear, best practices and next steps are recommended. The solutions team guided tasks that can be included in a migration are:

- **Custom workflow creation**—Creation of custom workflows that automate the signing process, reducing errors and delays. From reusable templates to Advanced Workflows for Adobe Sign, workflows increase the speed of the signing process and business.
- **Widgets**—Widgets are reusable [e-signature](#) components that can be embedded into web pages or websites to improve customer experience.
- **Integrations**—Adobe Sign marketing-leading integrations enable you to integrate [electronic signatures](#) directly into the enterprise applications your organization relies on every day. These can include Salesforce, SharePoint, Microsoft Dynamics, NetSuite, Workday, and others.
- **API consulting**—Using API consulting, you can build Adobe Sign access and integration directly into your custom business applications. Integrations allow you to start the signing experience entirely from within an external application or incorporate functionality into external applications.

Summary.

Bringing Adobe Sign to your organization delivers new levels of agility, efficiency, cost savings, and superior customer experiences. Adobe is laser focused on partnering with you as you make this critical investment to create, develop, deploy, and optimize your implementation. Migration services are designed to ensure that each customer receives Adobe's world-class services to ease onboarding to Adobe Sign.



Adobe, the Adobe logo, and Acrobat are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2017 Adobe Systems Incorporated. All rights reserved.



Adobe Sign for Microsoft Office 365

Accelerate workforce productivity and securely transact business with Adobe e-signatures.

Manual processes have no place in today's fast-paced competitive marketplace. [Adobe Sign](#) adds powerful e-signature capabilities to the full suite of Office 365 software to automate approval workflows right from the tools your teams use every day. As Microsoft's preferred signature provider, Adobe Sign integrates seamlessly with multistep processes in SharePoint and Flow as well as standalone workflows in Outlook, Word, PowerPoint, and Teams. Now there's an easy way to send documents for signature, track their status, and collect data, without leaving the Microsoft applications your company relies on.

Save time and speed signing.

Adobe Sign makes it fast and easy to collect [e-signatures](#) on any document, form, or contract directly from the Office 365 apps you use every day. From complex business processes to one-off approvals, Adobe Sign fits into all your Microsoft workflows:

SharePoint—Merge customer data and documents from SharePoint into electronic contracts, and create workflows based on business logic to route those contracts for signature. For example, you can set up a SharePoint workflow that automatically routes contracts valued at less than \$100,000 to a single approver and contracts valued at more than \$100,000 to multiple approvers.

Outlook—Initiate the signing process for agreements right from your favorite email app by clicking Send For Signature in the Outlook taskbar. Automatically track approval progress along the way. And even use Fill and Sign to automatically create form fields, and complete and approve documents that are sent to you.

Word and PowerPoint—Create estimates and contracts from scratch, send them for approval, and monitor progress in real time directly from the apps.

"We, as a state, use SharePoint in almost everything. So having Adobe Sign being flexible enough to be a module part of SharePoint—having that all under one roof—has made that easier for us."

MICAH HWANG

Service delivery specialist,
State of Hawaii

Use cases

Adobe Sign can automate Office 365 document workflows across your organization.

Sales

- Contracts
- Work order authorizations
- Estimates
- Change orders
- Renewal agreements
- Invoices
- Supplier agreements

Human resources

- Employment applications
- Offer letters
- Training compliance forms
- Contractor agreements
- Benefits enrollment
- Payroll forms
- Separation agreements

Internal workflows

- Document approvals
 - Audits
 - Nondisclosure agreements (NDAs)
 - Internal forms
 - Proposals
 - Credit card authorizations
 - Government forms
-

Microsoft Flow—Incorporate e-signatures into your favorite Microsoft Flow applications, and automatically kick off tasks after an agreement is signed.

Microsoft Teams—Collaborate with colleagues to create and send agreements, and send those documents for signature using Adobe Sign bots.

Deliver exceptional customer experiences.

Whether you're integrating e-signatures into smart SharePoint workflows, quickly requesting approvals from Outlook, or using another Microsoft app to send and track contracts, your clients, customers, and partners will love the signing experience. When a document is ready to be signed, recipients get an email with a link. They can click or tap the link from any browser or mobile device—no matter where they are—and easily sign in seconds. There's no need to install additional software. An intuitive wizard guides recipients to each required field, and they simply type their name to sign.

"Our executives were very pleased with the speed of Adobe Sign. Signed contracts are delivered to their email inboxes in an average of two days instead of four weeks."

COR VAN DER SCHEER

Procurement processes and
systems manager,
AusNet Services

Protect your documents and data.

One of the advantages of a trusted e-signature solution is the security it brings to your information management workflows. Adobe Sign delivers more than 1,000 security features, processes, and controls to protect the documents and data that flow through your organization. Increase signing security for sensitive documents with multifactor authentication or certificate-based [digital signatures](#). Rely on e-signature technology that complies with rigorous global security standards, such as ISO 27001 and SOC 2 Type 2. And improve compliance by archiving signed documents with a complete audit trail.

Maximize productivity with industry leaders.

Join the ranks of industry and government leaders—including AusNet and the state of Hawaii—that are using Adobe Sign and Office 365 to accelerate document workflows and secure transactions. As preferred enterprise solution partners, Adobe and Microsoft are partnering to develop integrated services across Adobe Document Cloud and Office 365 that help businesses digitally transform while delivering great experiences for their customers.



Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2017 Adobe Systems Incorporated. All rights reserved.

ISO/IEC 27001:2013 Information Security Management Certificate of Approval

Awarded to:

Adobe Systems Incorporated

The scope of
approval:

Adobe's Information Security Management System (ISMS), in accordance with the requirements of ISO standard ISO/IEC 27001:2013, is to appropriately preserve the Confidentiality, Integrity and Availability (CIA) of the platforms, services and applications that are used in processing, transmitting and storing customer assets and/or Personally Identifiable Information for the following enterprise offerings:

- Adobe Marketing Cloud
- Adobe Managed Services
 - Experience Manager
 - Connect
 - Creative Cloud for enterprise
- Adobe Document Cloud
- Adobe Creative Cloud for enterprise
- Adobe Captivate Prime

This is in accordance with the Statement of Applicability version 1.0.

Statement of
applicability:

Version: 1.0

Locations in scope:

345 Park Avenue, San Jose, CA 95110-2704, USA

Signed:
For KPMG Audit plc



Certificate issue &
number:

Date: 30th November 2016 Certificate Number: 630

N.B. Certificate remains valid while accompanied by current schedule of approval bearing the same certificate number.

Validity of this certificate can be verified by contacting kpmgcertificationservices@kpmg.co.uk with your query.

© 2016 KPMG Audit plc, a public limited company and a member firm of KPMG International, a Swiss cooperative. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

This certificate provides verification in accordance with ISO/IEC 27001:2013. It does not constitute an assurance opinion delivered in accordance with IAASB Assurance Standards

Registered office: 15 Canada Square, London, E14 5GL.

UKAS accredited office: One Snowhill, Snow Hill Queensway, Birmingham, B4 6GH

ISO/IEC 27001:2013 Information Security Management Schedule of Approval



137

www.kpmg.co.uk

Awarded to:

Adobe Systems Incorporated

The scope of
approval:

Adobe's Information Security Management System (ISMS), in accordance with the requirements of ISO standard ISO/IEC 27001:2013, is to appropriately preserve the Confidentiality, Integrity and Availability (CIA) of the platforms, services and applications that are used in processing, transmitting and storing customer assets and/or Personally Identifiable Information for the following enterprise offerings:

- Adobe Marketing Cloud
- Adobe Managed Services
 - Experience Manager
 - Connect
 - Creative Cloud for enterprise
- Adobe Document Cloud
- Adobe Creative Cloud for enterprise
- Adobe Captivate Prime

This is in accordance with the Statement of Applicability version 1.0.

Statement of
applicability:

Version: 1.0

Locations in scope:

345 Park Avenue, San Jose, CA 95110-2704, USA

Signed:
For KPMG Audit plc

Certificate validity:

Date: 30th November 2019

N.B. Certificate remains valid while accompanied by current schedule of approval bearing the same certificate number.

Validity of this certificate can be verified by contacting kpmgcertificationservices@kpmg.co.uk with your query.

© 2016 KPMG Audit plc, a public limited company and a member firm of KPMG International, a Swiss cooperative. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

This certificate provides verification in accordance with ISO/IEC 27001:2013. It does not constitute an assurance opinion delivered in accordance with IAASB Assurance Standards

Registered office: 15 Canada Square, London, E14 5GL.

UKAS accredited office: One Snowhill, Snow Hill Queensway, Birmingham, B4 6GH



An official website of the United States government



<https://www.fedramp.gov>

Products

Agencies

Assessors



1
Authorizations

Adobe - Adobe Document Cloud (PDF Services & Adobe Sign)



FedRAMP Ready



FedRAMP In Process



FedRAMP Authorized

FedRAMP Authorized Since 05/14/2018

System Profile

Service Model

SaaS

Deployment Model

Public Cloud

Impact Level

Li-SaaS

Contact Information

POC: Paul Faust

E-mail: fedramp@adobe.com (mailto:f...

Website: <https://acrobat.adobe.com> (...)

Package ID

FR1820435961

[Package Access Request Form \(https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2017/02/FedRAMP-Package-Request-Form_V5_03012017.pdf\)](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2017/02/FedRAMP-Package-Request-Form_V5_03012017.pdf)

FedRAMP Authorization Details

Authorization Type: Agency

Independent Assessor: General Services Administration

Agency Authorization Date: 05/14/2018

FedRAMP Authorization Timeline

04/23/2018

In-Process

05/14/2018

Authorized

Service Description

—

Adobe Document Cloud is a complete portfolio of secure digital document solutions that speeds business and drives better customer experiences by making manual, paper-based processes 100% digital. Document Cloud includes PDF Services and Adobe Sign along with web and mobile apps that can be used standalone or integrated into your organizations' existing document processes, business applications, or enterprise systems.

Additional products from this provider

[Adobe Connect Managed Services \(ACMS-EW\)](#)

[Adobe Connect Managed Services \(ACMS-GC\)](#)

[Adobe Creative Cloud for enterprise](#)

[Adobe Experience Manager Managed Services \(AEMMS-EW\)](#)

[Adobe Experience Manager Managed Services \(AEMMS-GC\)](#)

Agencies using this service

[Broadcasting Board of Governors](#)

Current List of Certifications, Standards, and Regulations

Adobe Service Offering	Completed Certifications and Attestations
Adobe Captivate Prime	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, GLBA-Ready ¹ , FERPA-Ready ¹
Adobe Connect On-Demand	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, GLBA-Ready ¹
Adobe Creative Cloud for enterprise	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, FedRAMP Tailored, GLBA-Ready ¹ , FERPA-Ready ¹
Adobe Document Cloud - Acrobat DC	SAFE BioPharma® digital identification standard
Adobe Document Cloud - Adobe Sign	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, FedRAMP Tailored, HIPAA-compliant ¹ , GLBA-Ready ¹ , FERPA-Ready ¹ , FDA 21 CFR Part 11 compliant ¹ , PCI DSS V3.2 compliant merchant and service provider, SAFE BioPharma® digital identification standard
Adobe Document Cloud - PDF Services	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, FedRAMP Tailored, GLBA-Ready ¹ , FERPA-Ready ¹ , PCI DSS V3.2 compliant merchant and service provider ⁴
Adobe Managed Services (Connect and Adobe Experience Manager (AEM) ² only)	FedRAMP, SOC 2–Type 2 (Security & Availability), ISO 27001:2013, GLBA-Ready ¹ , FERPA-Ready ¹ , HIPAA-compliant ¹
Adobe Experience Cloud (all solutions) ³	SOC 2–Type 2 (Security & Availability), ISO 27001:2013, GLBA-Ready ¹
Adobe.com eCommerce	PCI DSS 3.2 compliant merchant

¹ An Adobe service that is GLBA–Ready, FERPA-Ready, FDA 21 CFR Part 11 compliant, or HIPAA compliant means that the service can be used in a way that enables the customer to help meet its legal obligations related to the use of service providers. Ultimately, the customer is responsible for ensuring compliance with legal obligations, that the Adobe service meet its compliance needs, and that the customer secures the service appropriately. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.

² AEM Mobile and AEM Livefyre are recent acquisitions and are not currently part of the AEM Managed Services offering.

³ Adobe Experience Cloud includes Adobe Analytics, Adobe Audience Manager, Adobe Campaign, Adobe Experience Manager, Adobe Media Optimizer, Adobe Prime Time, Adobe Social, Adobe Target

⁴ PCI DSS compliance excludes Adobe Send & Track service.



Signed document encryption



SIGN ▾

Search Adobe Support



Sign In

Search

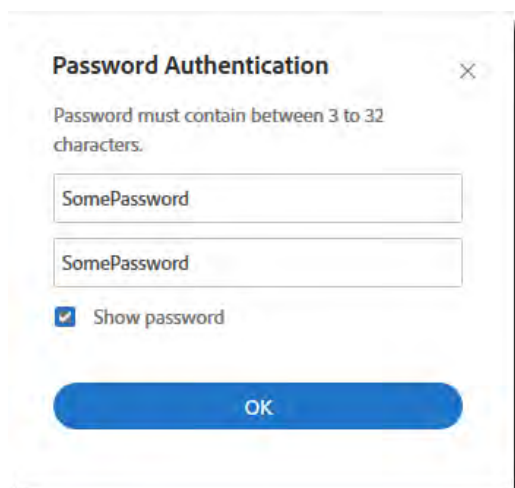
Agreement encryption methods

When sending an agreement, you can set options on the Send page to either verify that the signer is indeed the correct person, or secure the signed, completed document with a password.

These methods of encryption add a level of security that keeps you and your signer's information safe.

✓ Verify signer identity using a password

This option allows the sender to set a specific password. You can then send that password to your signer, (outside Adobe Sign, for example, by regular email or via phone) to allow them to access and sign the document.



A screenshot of a 'Password Authentication' dialog box. The title bar says 'Password Authentication' with a close button (X). Below the title, it says 'Password must contain between 3 to 32 characters.' There are two text input fields, both containing 'SomePassword'. Below the fields is a checkbox labeled 'Show password' which is checked. At the bottom is a blue 'OK' button.

Note:

Passwords can only contain letters and numbers; no special characters are allowed.
For example:

` ~ ! @ # \$ % ^ & * () _ + - = [] \ ; ' , . / { } | : " < > ?

Note:

It is important to remember the Signing password you set as it is not possible to recover, or reset this password in any way. If the signing password is lost or forgotten, there is no way to access the document, or the transaction in any way. If the document is inaccessible, the sender needs to cancel that transaction and send the document again.

✓ Password protect the signed document

This option allows the sender to set a specific password that is applied to the Signed PDF document. This password is required to open and view the Signed PDF file.

Checking the **Show Password** checkbox exposes the content of the password field to help ensure the two are correct, and what you intend.

If the two passwords do not match, an error icon appears in the second password field.

Dashboard **Send** Manage Reports Account Casey ▾

Recipients

Complete In Order ☐ Complete In Any Order ☒ Add Me Add Recipient Group ?

1	jupiter@jupiter.dom	Email		
2	Enter recipient email			

[Show CC](#)

Message

GlobalCorp Client Services Agreement

Please review and complete GlobalCorp Client Services Agreement.

Files [Add Files](#)

GlobalCorp Client Services Agreement.pdf

Drag More Files Here

Options ?

☒ Password Protect

Password must contain between 3 to 32 characters.

SomePassword123

SomePassword12

☒ Show password

☐ Completion Deadline

☐ Set Reminder

Note:

Passwords can only contain letters and numbers; no special characters are allowed.
For example:

` ~ ! @ # \$ % ^ & * () _ + - = [] \ ; ' , . / { } | : " < > ?

Note:

It is important to remember the Signed PDF password you set is embedded into the PDF, and is not possible to recover or reset.

If the Signed PDF password is lost or forgotten, there is no way to open the PDF.

Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)[< See all apps](#)[Learn & Support](#)[Get Started](#)[User Guide](#)[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

Transform business processes with electronic and digital signatures.

Adobe Sign lets you comply with local and international regulations using one scalable signature solution.

A White Paper

September 2017

TABLE OF CONTENTS

3	Transforming the way you sign on the dotted line.
4	Electronic vs. digital signatures: What's the difference?
5	The ins and outs of electronic signature laws.
6	Choosing the right approach for your processes.
8	One solution. Multiple options.
9	Comparing signature types in Adobe Sign.
10	Adobe: The digital document leader.
11	Resources

Transforming the way you sign on the dotted line.

Organizations around the world are urgently transforming their businesses, using digital technologies to deliver agility, efficiency, cost savings, and great customer experiences. Document signature processes represent one of the biggest opportunity areas to accelerate this shift. Workers spend countless hours hunting down approvals and ink signatures—and then print, scan, fax, or mail documents to get the job done. The resulting delays frustrate customers, business partners, and employees alike—and ultimately reflect poorly on the company's brand.

It's little wonder that organizations have embraced electronic and digital signatures. Today, leading companies in every industry and geography—including KLM, Groupon, Jaguar Land Rover, Ricoh, Unum, and LeasePlan Corporation—get fast, legal, and secure signatures electronically. The results are impressive. Ricoh accelerated turnaround time for sales contracts and trimmed five days off the process. LeasePlan reduced its average contract turnaround

time from 23.5 days to 4 days and 2 hours—an 83% reduction in processing time.

The biggest question today isn't whether to adopt [electronic signatures](#)—it's how to go about it.

While the terms may seem similar, electronic and digital signatures actually describe two different approaches to signing documents—and those differences are linked with signature laws and regulatory requirements. To make the right choice for your organization, you'll want to learn about those differences, understand your unique legal or regulatory environment, and partner with a company you trust—to help you deliver value today and into the future.

This paper explores electronic and digital signatures and shows how Adobe solutions let you work with either approach, or a combination of the two. [Adobe Sign](#) is an Adobe Document Cloud solution that manages signature processes from end to end,

integrates easily with existing business processes, and provides a quick return on investment. With over 20 years of experience developing and refining PDF and signature technologies, Adobe is uniquely positioned to help you build legal and compliant signature processes.

"The courts now recognize an advanced e-signature solution with high security and privacy standards like Adobe Sign. We've partnered with Adobe and created a set of best practices in the area."

BART VAN DEN HEUVEL
Manager of corporate procurement
LeasePlan Corporation

Electronic vs. digital signatures: What's the difference?

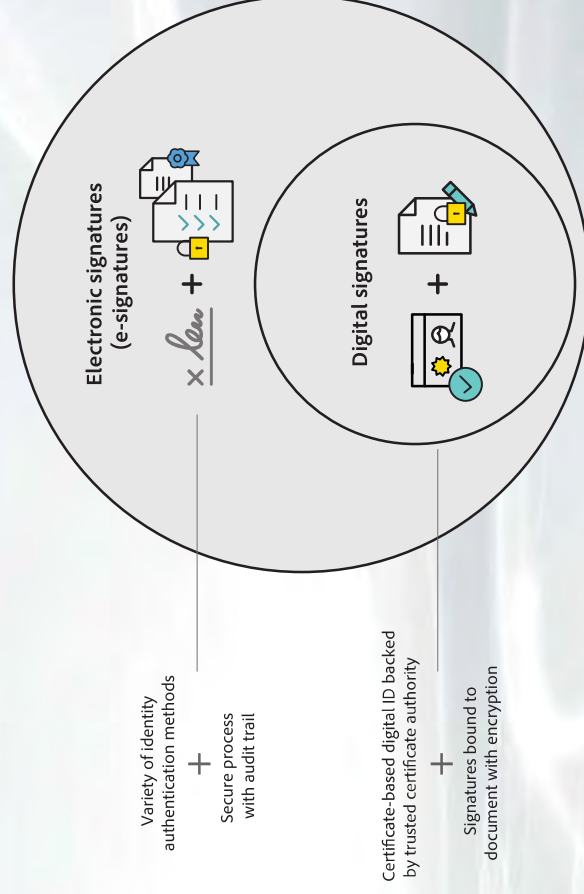
Electronic signatures (e-signatures) refer to any electronic process that indicates acceptance of an agreement or a record. Electronic signatures:

- Use a variety of common electronic authentication methods to verify signer identity, such as email, social IDs, passwords, or a phone PIN. Standard e-signatures use single factor authentication. Enhanced e-signatures use multifactor authentication to increase security when needed.
- Demonstrate proof of signing using a secure process that often includes an audit trail along with the final document.

Digital signatures use a specific method to sign documents electronically. Digital signatures:

- Use a certificate-based digital ID to authenticate signer identity.
- Demonstrate proof of signing by binding each signature to the document with encryption—validation is done through trusted Certificate Authorities (CAs) or Trust Service Providers (TSPs).

Electronic signature types



The ins and outs of electronic signature laws.

Electronic signatures are legally binding in nearly every industrialized nation, and even less developed countries are beginning to enact e-signature laws. In 2000, the United States passed the Electronic Signatures in Global and National Commerce (ESIGN) Act, making e-signatures legal for virtually all uses. In the European Union, the Electronic Identification and Trust Services (eIDAS) regulation took effect in July 2016. It established a new legal structure for electronic identification, signatures, seals, and documents—creating a single digital market across the entire EU. To learn more about signature laws, read [Global Guide to Electronic Signature Laws: Country by Country](#).

The right approach to building a compliant electronic signature process for your business will depend on your unique regulatory environment, risk profile, and specific business requirements. There's a marked contrast, for example, in legal approaches between the United States and the European Union. U.S. law allows

for a broad definition of electronic signatures and does not prescribe a specific technology. In contrast, the EU eIDAS regulation distinguishes between three types of electronic signature approaches, and requires digital signatures for some types of documents. In addition, some business sectors, such as biopharmaceutical and government, have developed more prescriptive guidelines for specific business processes that require digital signatures.

Worldwide, there are generally two types of electronic signature laws:

Minimalist laws—Many countries, including the United States, Australia, New Zealand, and Canada, have minimalist or permissive laws, which allow for the broad enforceability of e-signatures with few legal restrictions and give e-signatures the same legal status as handwritten signatures.

Multi-tier laws—Countries with multi-tier laws generally permit the broad use of e-signatures but provide greater evidentiary weight to signatures that use different types of certificate-based digital IDs to authenticate signers. Regions and countries that have adopted multi-tier laws include the European Union, China, India, and South Korea. In the European Union, for example, only signatures using digital IDs from qualified providers are automatically given the same status as handwritten signatures.

Choosing the right approach for your processes.

To find the right signature approach for your business, you'll need to balance regulations and risk, and consider what level of effort is necessary to make your business transactions both legal and secure. In general, properly configured e-signature processes are easier to implement, and meet legal and security requirements for many business processes. Digital signatures have additional technical demands, but provide an advanced form of authentication that meets more stringent requirements. Adobe Sign supports both approaches in one flexible, scalable solution, letting you choose one or the other—or a combination of the two.

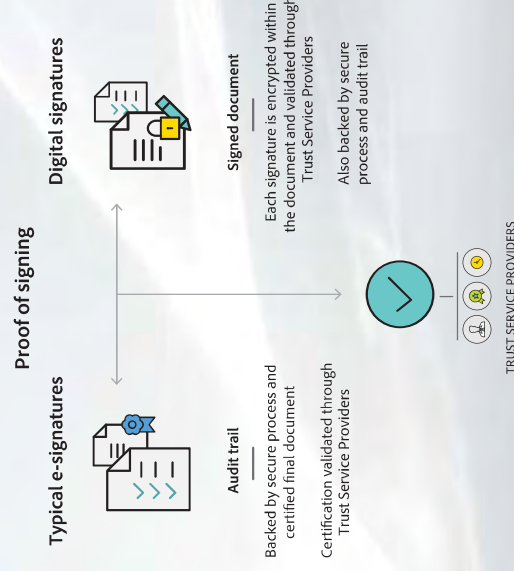
Typical signer authentication for everyday approvals.

E-signature processes in Adobe Sign are compliant with e-signature laws, such as the U.S. [ESIGN Act](#) and EU eIDAS regulation. With support for both single factor and multifactor authentication, Adobe Sign gives you a range of options to verify signer identities. Standard authentication is achieved by sending an email request and private link to a specific person. Because most signers have unique access to one email account, this is considered the first level of authentication. To strengthen

security and help prevent hackers from spoofing the system, you can use "enhanced authentication," which adds another verification step before signers open the document. Senders can choose from a variety of methods—such as social IDs, passwords, phone PINs, and knowledge-based authentication (KBA)*—to reconfirm the signers' identity. To further improve legal compliance, you can also build processes that require an explicit consent to do business electronically before engaging in the signature process.

Adobe Sign manages the document securely throughout the process and certifies the signed document with a tamper-evident seal to confirm its integrity. Each key step in the signature process is logged, such as: when the agreement was sent, opened, and signed; IP addresses or geolocations of signers; and the specific form of authentication used for each signer or approver.

The result is captured in a secured audit trail. Both the signed document and audit trail are delivered to all parties and securely stored in Adobe Document Cloud, providing clear, easily producible evidence of each party's signature.



"Our average turnaround time for signed contracts with Adobe Sign is 1.3 hours. Considering that it used to take at least two weeks, and sometimes even months with paper contracts, this is a huge improvement."

Western Australian Local Government Association (WALGA)

* Knowledge-based authentication available in the United States only.

Robust authentication for stricter requirements.

Digital signature processes in Adobe Sign are compliant with more rigorous requirements, such as advanced (AdES) and qualified (QES) electronic signatures in the EU eIDAS—and provide comprehensive support for working with accredited Certificate Authorities (CAs) and Trust Service Providers (TSPs). They also work with qualified signature creation devices (QSCDs), such as smart cards, USB tokens, and cloud-based hardware security modules (HSMs).

Documents signed digitally in Adobe Sign provide evidence of each participant's signature within the document itself. During the signing process, the signer's certificate is cryptographically bound to the document using the private key uniquely held by that signer.

During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signer's identity through the CA and help ensure no changes were made to the document since it was signed. Audit trails can also provide additional, valuable information such as the signer's IP address or geolocation.

Understanding Trust Service Providers.

To achieve the highest levels of security, digital signature processes use a technology approach called Public Key Infrastructure (PKI) for encryption, signing, and certificate authentication. Digital IDs are issued by CAs and TSPs that meet defined requirements. These providers, in turn, are part of a standards-based, industry-wide effort to allow verification of signer identities and document authenticity on a global scale.

Industries and governments publish lists of authorities that meet defined requirements. Adobe uniquely enables global validation for the entire industry through publication and management of trusted lists. Global and regional lists, like the [Adobe Approved Trust List \(AATL\)](#) and the [European Union Trusted Lists \(EUTL\)](#), are fully supported in Adobe solutions.

Trust Service Providers offer a range of secure identity and transaction services, including:

- Registration Authority (RA)—Signer identities are verified to qualify for an ID.
- Certificate Authority (CA)—Once verified, a CA issues a private key and the corresponding certificate, and then manages it over time. The private key is controlled by a password or PIN uniquely known to the signer.
- Time Stamp Authority (TSA)—Digital signature processes also engage with TSAs to establish an accurate time for each signing event.

Adobe Sign lets you work with your choice of TSPs to sign and time stamp documents, so you can comply with laws or regulations governing your specific country or industry. During the validation process, Adobe also confirms that the authorities being used in the document are trusted providers—approved through global, regional or industry-specific accreditation. Trust lists, such as AATL and EUTL, serve the entire industry, providing an authoritative source of Trust Service Providers. Examples of participants include:

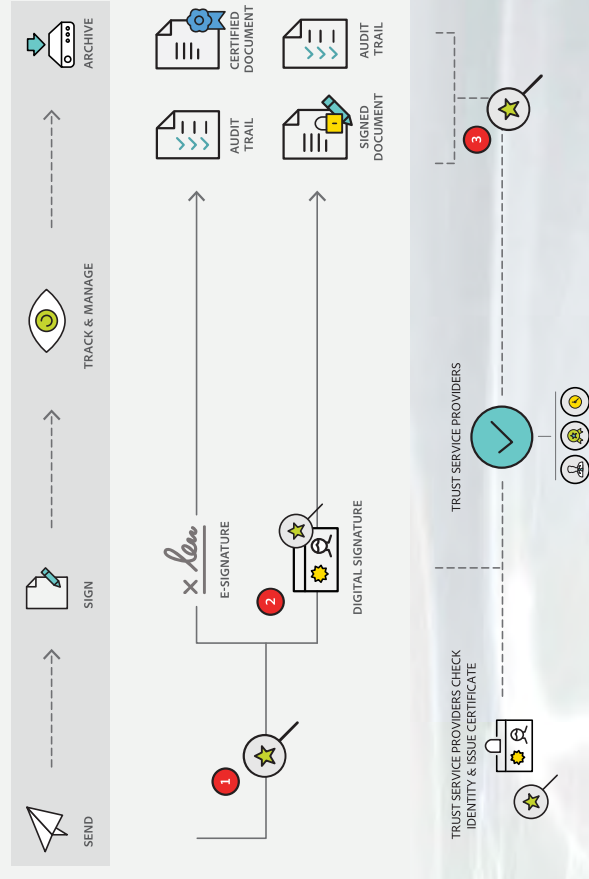
- The U.S. federal government and Department of Defense
- All 28 member states of the European Union
- The governments of Japan, Brazil, Switzerland, India, and Uruguay
- Postal services of Germany, France, Italy, Hong Kong, and South Africa
- SAFE-BioPharma and IdenTrust

One solution. Multiple options.

Adobe Sign is uniquely designed to support the broadest range of electronic and digital signature requirements, so you can do business locally or globally—and choose the best approach for each of your business processes. With Adobe Sign, you can build end-to-end workflows that include typical e-signatures, digital signatures, or both. Adobe Sign also provides industry-leading support for signer authentication and validation.

- 1 Before opening your document, signers authenticate their identity using single factor or multifactor methods.
- 2 Signers add digital signatures using a password or PIN-protected private key from their certificate to bind their signature to the document.
- 3 Signer and document authenticity are validated through trusted providers.

E-signatures and digital signatures in Adobe Sign



"With Adobe Sign, instead of it taking a day to send out a policy form on paper and then waiting a week or longer for the completed form to come back, 70% of returned forms are received within 24 hours. The process is easier all around and translates to a much better customer experience."

CHRISTINE FRANCIS
Business operations development
manager of shared services
Unum

Comparing signature types in Adobe Sign.

Whether your signers use e-signatures or digital signatures, Adobe Sign supports essential requirements to help you build fully compliant business processes.

		Typical e-signatures	Digital signatures
Consent to e-sign	Explicit consent can be captured during the process	✓	✓
Authenticate	Single factor e-signature authentication with email ID and a secure, tracked process	✓	✓
	Enhanced, multifactor e-signature authentication (e.g., email plus social ID, phone PIN, knowledge based, password, and more)	✓	✓
	Digital signature authentication with digital ID and private PIN	—	✓
Sign	E-sign using a web browser or mobile device. No downloads or signups required.	✓	✓
	Sign with a digital ID using your desktop computer. Work with smart cards, USB tokens, HSMs, and over 200 CAs globally.	—	✓
	Sign with a cloud digital ID using your web browser or mobile device. Take advantage of open standards for cloud-based digital signatures.	—	✓
	Built-in or third-party TSA	✓	✓
Time stamp			
Ensure document integrity	Certified by Adobe	✓	✓
	Digitally signed by all participants	—	✓
Track all events	Audit trail certified by Adobe	✓	✓
Validate through Trust Service Providers	Tamper-evident seal	✓	✓
	Time stamp	✓	✓
	Signer's identity and signature	—	✓
Secure the process	ISO 27001, SOC 2 Type 2, PCI DSS certification and Adobe SPLC compliance	✓	✓
Comply with regulations	Complies with HIPAA, FERPA, GLBA, and other privacy regulations around the world	✓	✓
	Supports compliance with Food and Drug Administration (FDA) 21 CFR Part 11	—	✓
Store data in your region	Data centers located in North America, Europe, Australia, and Japan	✓	✓

Adobe: The digital document leader.

With 6 billion transactions a year, Adobe is the global leader in secure digital document solutions and standards-based electronic signatures. With flexible signature approaches, the easiest signing experience, unparalleled integrations, and superior workflow, Adobe Sign is the ideal choice for building great employee and customer experiences while ensuring full compliance with local and global signature laws. We're trusted and used by Fortune 1000 companies, government, healthcare, and financial institutions to help automate signing and approvals across a wide range of departments and business processes.

Key benefits of Adobe Sign

Standards-based signing—We invented PDF— and the digital signatures that work in PDF— then worked with industry-recognized standards organizations ISO and ETSI to turn them into open standards. Adobe solutions work with over 200 CAs around the world, and we're the only global vendor to support every European Union TSP accredited to issue qualified digital IDs. We're also advancing an open standard for cloud-based digital signatures with the Cloud Signature Consortium—so anyone can digitally sign documents from anywhere while meeting the highest security standards.

World-class capabilities—Adobe Sign makes it easy to manage end-to-end business processes. Quickly send documents out for signature and get the job done in record time. Documents are stored in your business system, a repository of your choice, or [Adobe Document Cloud](#)—and backed by strict security, so your employees can store, access, track, and manage documents from anywhere in real time.

Maximum flexibility—Use one single, scalable solution to create end-to-end signing processes that include digital signatures, e-signatures, or a combination of the two. Adobe Sign gives you flexibility to build workflows in accordance with your specific compliance, industry and risk profile. Build digital signature processes using the CA or TSP of your choice with support for the full range of signature creation devices including smart cards, USB tokens and cloud-based HSMs.

Comprehensive security controls—Adobe takes the security of your digital experiences very seriously. Adobe Sign meets rigorous security standards—including ISO 27001, SOC 2 Type 2, and HIPAA, as well as PCI DSS used in the Payment Card Industry. We also employ Adobe Secure Product Lifecycle (SPLC) practices, a demanding set of several hundred specific security activities—spanning software development practices, processes, and tools—integrated into multiple stages of the product lifecycle.

An enterprise-grade solution—Powerful administration tools in Adobe Sign help you manage user and group preferences, restrictions, and languages quickly and easily. Ultra-high availability data centers in North America, Europe, Australia, and Japan keep business running smoothly. All administrative data, document processing, and document data and metadata remain in that region or country for the entire data lifecycle.

Superior prebuilt integrations—Easily add electronic signatures that work natively in your systems of record with richly featured, preintegrated solutions. Adobe Sign integrations and robust APIs let you embed signature processes within your organization's enterprise systems and applications. Integrations include Salesforce, Workday, Microsoft Dynamics CRM, Ariba, SAP, Apptus, and more.

Exceptional customer experience—Delight customers with fast response times and speedy contract signing processes. Customers can sign without printing or faxing documents, installing software, creating new logins, or scanning anything. The entire process can take just minutes from start to finish, so everyone can finish quickly and get on with their day.

To learn more about how Adobe Sign can benefit your organization, contact your Adobe sales representative today.

Resources

Discover even more by consulting these additional resources:

- Adobe Sign Solution Brief
- Global Guide to Electronic Signature Law: Country by country
- Developing an effective electronic signature policy

For more information

Solution details:

<https://adobe.com/go/adobesign>



Copyright © 2017 Adobe Systems Incorporated. All rights reserved.
Adobe and the Adobe logo are either registered trademarks or
trademarks of Adobe Systems Incorporated in the United States
and/or other countries.



Sign In



SIGN ▾

View the agreement audit trail

Search Adobe Support



Search

See the history of a transaction

Once a transaction is sent, you can see who performed what action and when in the agreement history. This information is updated as each new event occurs and provides details on each event.

Applies to: **Sign**Last Published: **August 25, 2017**

▼ Quick steps:

1. Go to the **Manage** page
2. Single-click a listed transaction to select it
3. Click the **History** tab on the right side of the page
4. Click the **Audit Report** link at the top-right of the history content

▼ Step-by-step:

1. Go to the **Manage** page
Single-click the agreement
Slick the **History** tab on the lower-right side of the page

The screenshot shows the Adobe Sign 'Manage' tab. At the top, there are navigation links: Dashboard, Send, Manage (active), Reports, and Account. A user dropdown menu shows 'Casey'. Below these are filters: 'Filter by Name or Company' and 'Filter by Document Status', followed by a search bar 'Search documents, recipients & notes'. The main table has columns: Name, Company, Document Title, and Date. It lists document statuses: 'Waiting For Me to Sign (0)', 'Out for Signature (1)', 'Signed (1)', and 'Archived (0)'. A red box highlights the document 'Jupiter Io' from 'Jupiter LLC' titled 'GlobalCorp Client Services Agre...' signed on '08/25/2017'. To the right of the table is a document preview for 'GlobalCorp Client Services Agreement' with details: From: Casey Jones (CaseyJones), To: Jupiter Io (Jupiter LLC), Date: 08/25/2017, 9:25 AM, Status: Signed. Below the preview is a 'History' section with an 'Audit Report' link highlighted in yellow. A red arrow points from the highlighted document row to the 'History' tab in the right-hand pane. The 'History' tab is also highlighted with a red box. Other tabs in the right-hand pane include View, Share, Protect, Remind, and Notes.

- 2 The history of events for the transactions appears in the information window.

Click the **Audit Report** link to open a PDF with more details, including IP addresses of where the events took place.

If the agreement contains form field the Export Data link downloads the form data in a .csv file.

History

[Audit Report](#)[Export Data](#)

- Document created by John Smith
(haringa@adobe.com)
Mar 31 1:39 pm
- Sent out for signature to test sign
(mytest@test.com)
Mar 31 1:39 pm
- Viewed by test sign (mytest@test.com)
Mar 31 2:19 pm
- Document e-signed by test sign
(mytest@test.com)
Signature Date: Mar 31 2:19 pm - Time
Source: server
Completed



Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)

**SIGN**[^ Back to top](#)[< See all apps](#)[Learn & Support](#)[Get Started](#)[User Guide](#)[Tutorials](#)**Ask the Community**

Post questions and get answers from experts.

[Ask now](#)**Contact Us**

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe

 [Change region](#) 

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

Adobe Cloud Services

Compliance Overview

Overview

At Adobe, the security, privacy and availability of our customers' data is our priority. We believe that a sound compliance and risk management strategy is as important to the success of an organization as the company's product strategy. To this end, our cloud strategy includes a two-pronged approach to keeping your data safer, more secure, and available.

To protect from the physical layer up, we implement a foundational framework of security processes and controls called the Common Controls Framework (CCF) by Adobe. CCF helps protect the Adobe infrastructure, applications and services, as well as helps us comply with a number of industry-accepted best practices, standards, regulations and certifications.

To protect from the software layer down, we use the Adobe Secure Product Lifecycle (SPLC), a rigorous set of several hundred specific security activities spanning software development practices, processes, and tools that are integrated into multiple stages of the product lifecycle.

Table of Contents

- 1 Overview
- 1 Which Standards Does Adobe Focus On?
- 4 Current State of Adobe Compliance
- 5 Conclusion

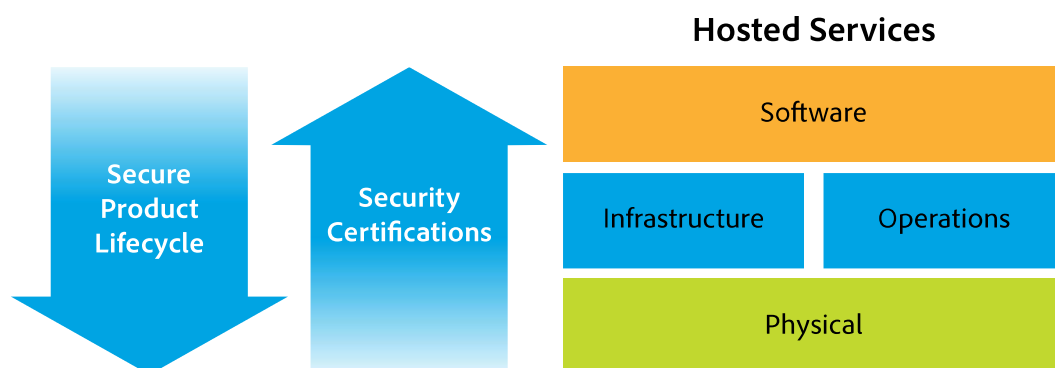


Figure 1: Adobe uses the Secure Product Lifecycle and Common Controls Framework to provide a complete view of compliance with industry standards and regulations.

Which Standards Does Adobe Focus On?

Adobe demonstrates our commitment to security by implementing a range of important industry standards and complying with government regulations concerning the security and privacy of data. While there are numerous industry standards and certifications comprising thousands of different requirements for compliance in the cloud, Adobe determined that significant overlap exists between these requirements and focuses on those that most significantly affect our customers. As new security standards and regulatory requirements are developed and adopted by the industry, Adobe will review them and adopt those with relevance to our customers. Depending on the focus of a particular Adobe service, it may comply with some or all of the following industry and regulatory standards.

Industry Standards

Adobe currently focuses on meeting the compliance requirements for the following primary industry standards.:

- **SOC**—The Service Organization Control (SOC) reporting standard has been established by the American Institute of Public Accountants (AICPA). Adobe currently utilizes the SOC 2 reporting standard. SOC 2 reports are based on a third-party attestation of compliance with AICPA Trust Service Principles (TSPs) relevant to security, availability, confidentiality, privacy, and processing integrity.

- **ISO 27001**—This certification demonstrates a systematic approach towards managing information security risks that affect the confidentiality, integrity, and availability of the service and customer information. ISO 27001 certification includes the establishment of a formal information security management program and demonstration of Adobe's commitment to providing transparency into its security controls and practices. ISO 27001 is of particular importance outside the United States.
- **FedRAMP**—The Federal Risk and Authorization Management Program (FedRAMP) is a collection of standards established by the U.S. Federal Government for security assessment, authorization, and continuous monitoring for cloud solutions. FedRAMP is mandatory for certain federal agencies. FedRAMP certification determines which cloud solutions can be purchased and deployed by federal agencies and their contractors.
- **PCI DSS**—The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle payment card information, such as credit card numbers. PCI DSS certification increases controls around cardholder data management. Being a PCI DSS-compliant service provider enables Adobe to help customers meet PCI requirements for the safe handling of personally identifiable data associated with a cardholder.

Regulatory Compliance

Adobe develops technologies and services that help our customers comply with their regulatory obligations. Customers are ultimately responsible for ensuring that their Adobe service is configured and secured in a manner that complies their legal obligations.

- **GLBA**—The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to safeguard their customers' personal data. A "GLBA-Ready" Adobe service means that the service can be used in a way that enables the customer to help meet its GLBA Act obligations related to the use of service providers.
- **HIPAA**—The Health Insurance Portability and Accountability Act (HIPAA) is legislation that governs the use of electronic medical records, and includes provisions to protect the security and privacy of personally identifiable health-related data called protected health information (PHI). By law, healthcare providers and insurance companies that have any sensitive PHI can only use products that are HIPAA-compliant. Certain Adobe services can be configured to be used in a way that supports HIPAA compliance by a customer that is a "covered entity" under HIPAA and signs Adobe's Business Associate Agreement (BAA).
- **21 CFR**—The Code of Federal Regulation, Title 21, Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11) establishes the U.S. Food and Drug Administration (FDA) regulations on electronic records and electronic signatures. Being 21 CFR Part 11 compliant means that Adobe services can be configured to be used in a way that allows pharmaceutical customers who engage with the FDA to comply with the 21 CFR Part 11 regulations.
- **FERPA**—The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. Student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.

Our Approach: The Common Controls Framework by Adobe

The Common Controls Framework (CCF) by Adobe is a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams. In creating CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe-specific controls that map to approximately a dozen industry standards.

**10+ Standards,
~1000 Control Requirements (CRs)**

**~ 273 common controls
across 20 control domains**

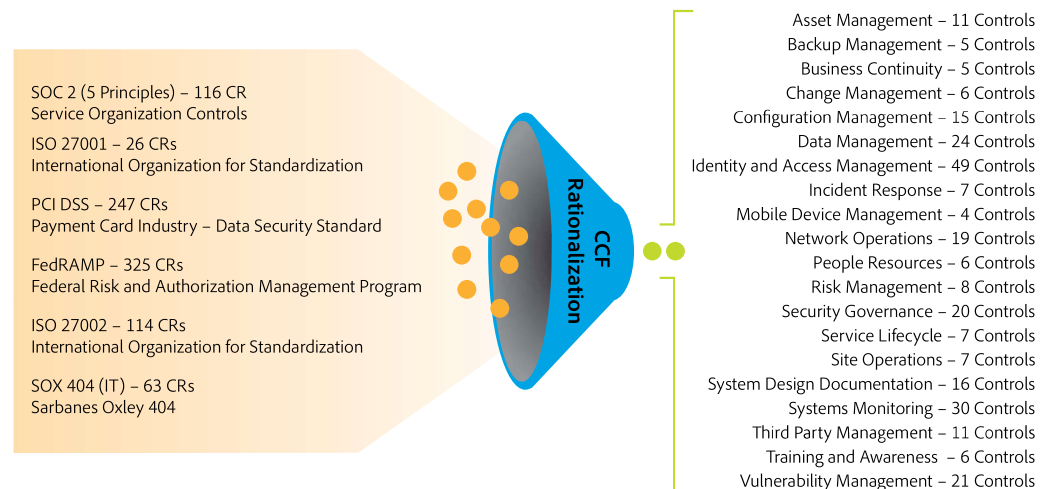


Figure 2: The Common Controls Framework by Adobe

Realizing that a product-specific, “siloe” compliance approach is neither cost-effective nor efficient, Adobe built CCF so that teams can inherit control capabilities from other parts of the organization. For example, software engineers are not responsible for data center security, however, they inherit the data center security capabilities from a data center operations team. This strategic simplicity enables the continuous execution of sustainable security controls.

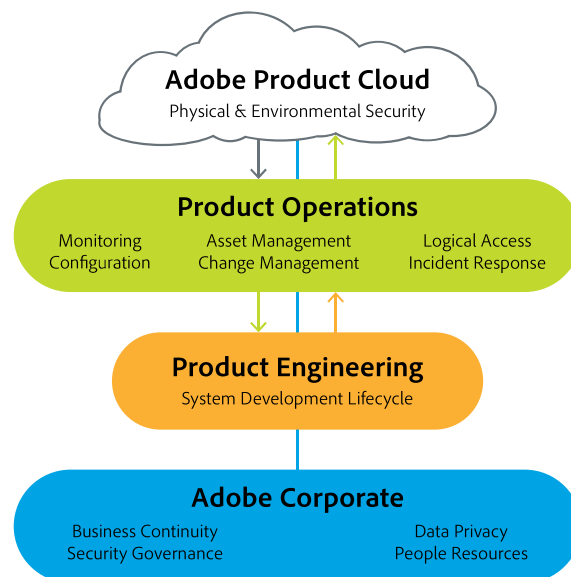


Figure 3: CCF by Adobe Conceptual Model

The Adobe SPLC aligns cleanly with CCF as well as industry best practices for software engineering teams to meet compliance requirements. A robust framework, the Adobe SPLC was designed from the ground up to include many controls that are now covered by CCF. Some of these controls include security testing (e.g., static analysis, dynamic analysis, penetration testing, etc.) and annual training of software engineers in secure coding techniques. While the SPLC was already used across all Adobe software engineering teams, the creation of CCF and the need to adhere to compliance requirements now helps ensure that the SPLC is more consistently applied throughout Adobe, thanks to improved process documentation and specificity.

Compliance requirements also impact the Adobe IT/Ops organizations, helping to ensure that key functions within asset management, business continuity management, change management, configuration management, backup management, network operations, data management, identity

and access management, and incident response are more rigorous and more consistently applied across the company. Some other areas also positively impacted by compliance requirements include data privacy controls for PII and PHI, logical access control for production and source code control systems, and the company's network security policy.

All Adobe personnel must participate in annual security awareness training as part of the compliance process. In addition, Adobe offers additional specific security training relevant to each employee's particular title and responsibilities. The compliance process also requires Adobe to formalize procedures throughout the company by documenting the procedure in advance, following the procedure to completion, and then providing evidence of the procedure's completion. For example, provisioning user access to a production environment requires a ticketed approval process in which the user's access to the environment must receive approval prior to provisioning. Adobe documents that procedure and the ticket is evidence of that documentation.

Adobe maintains ongoing compliance with periodic reviews, typically every quarter. These reviews include assessments of access to production systems, vulnerabilities, and firewall rules. More than 40 teams within the company have been trained in how to conduct a quarterly security review, including what to review, the process for a full review, and how to preserve evidence of the review.

Adobe uses an enterprise-wide governance, risk, and compliance (GRC) solution to establish an effective governance model for the compliance program. This solution enables automated metrics reporting and dashboarding, auditing, risk assessments, and issues and remediation tracking of all compliance controls. In addition, Adobe implements a periodic control, process, and risk self-assessment program that allows corporate management to evaluate compliance risks and certify the operating effectiveness of compliance processes and controls. The GRC solution provides an effective mechanism for management and auditors to establish ownership and accountability over the compliance program and monitor its operating effectiveness on a continuous basis.

The Adobe Common Controls Framework process doesn't end with the achievement of certifications and compliance with standards. Instead, the CCF is a continuous process that includes periodic internal audits, external assessments and on-going controls improvement. And because it is designed with flexibility in mind, the CCF allows us to quickly and easily adapt to new standards and changing requirements as well as international and regional requirements.

Current State of Adobe Compliance

To help ensure a consistent, company-wide strategy for all cloud offerings and platform services, Adobe has created a comprehensive compliance plan. With this plan, each team across the company documents the security and privacy controls it will implement, then the team implements the documented controls, and conducts regular, ongoing audits to prove compliance.

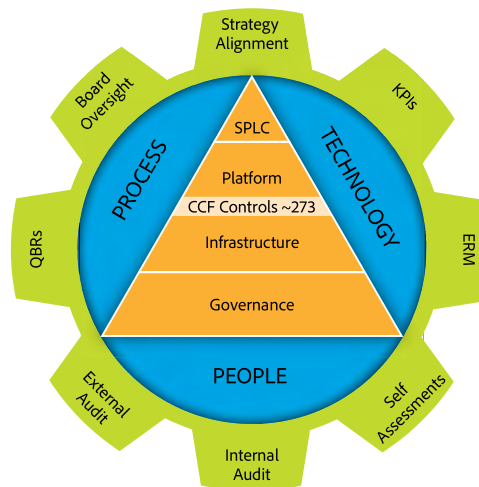


Figure 4: Adobe has created a comprehensive governance model to help ensure that security controls are operative, effective and monitored on an on-going basis.

Adobe Compliance

In addition to the certifications and compliance achievements already in place, additional efforts are in process and at various phases, according to the overall CCF by Adobe implementation. The most current list of all certifications for Adobe products and services [can be found on adobe.com](http://www.adobe.com).

Third-Party Compliance Audits

SOC 2

A leading accounting firm issued the Service Organization Controls (SOC2) Type 2 report after reviewing the suitability of the design and operating effectiveness of controls for Adobe's enterprise clouds relevant to meet the criteria for the Security and Availability principles set forth in TSP section 100, Trust Services Principles, and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA Trust Services Principles and Criteria)

Auditors from the accounting firm conducted their examination (over a period of 12 weeks) in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Auditor's procedures included testing the operating effectiveness of the required controls to provide reasonable assurance that the application Security and Availability principles were met.

ISO/IEC 27001:2013

The accounting firm also issued ISO/IEC 27001:2013 Information Security Management Certificate of approval after reviewing that Adobe's Information Security Management System (ISMS) is in place in accordance with the requirements of ISO standard ISO/IEC 27001:2013 to appropriately preserve the Confidentiality, Integrity and Availability (CIA) of the platforms, services and applications that are used in processing, transmitting and storing customer assets and/or Personally Identifiable Information within Adobe's enterprise cloud offerings.

SOC 2 reports and ISO/IEC 27001:2013 certificates are available through your Adobe sales representative.

Conclusion

The Common Controls Framework by Adobe is a central part of our company-wide security strategy. With the people, processes and technology, as well as a range of oversight, audit and follow-up mechanisms in place, Adobe ensures that CCF is not just a point in time; it's an ongoing commitment to help protect our customers and their data.

Please visit the Adobe security information site at <http://www.adobe.com/security> for more information about security efforts across our products and services.



Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative. Further details on Adobe solutions, including SLAs, change approval processes, access control procedures, and disaster recovery processes are available.

www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 12/2017 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

Adobe Sign technical overview

Security, compliance, identity management, governance, and document handling



Table of contents

- 1: Executive summary
- 2: Architecture
- 4: Identity management
- 4: Document certification
- 5: Security
- 8: Compliance
- 9: Operations
- 11: For more information

Executive summary

[Adobe Sign](#) is a Document Cloud solution that helps your organization deliver end-to-end digital document experiences with trusted, legal electronic signatures. Use Adobe Sign to easily initiate, sign, track, manage, and archive digital documents from web or mobile apps—or from within enterprise systems. Adobe Sign complies with many regional regulations and industry standards, and is accessible anywhere on any device. A robust cloud-based service, Adobe Sign securely handles large volumes of [electronic signature](#) (e-signature) processes, including:

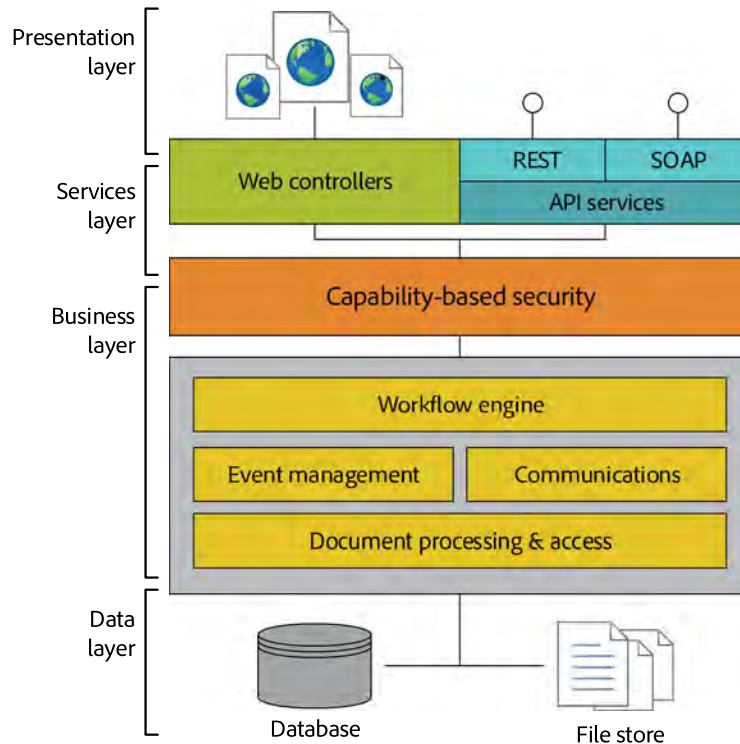
- Managing user identities with capability-based authentication
- Certifying document integrity
- Verifying e-signatures
- Logging recipient acceptance or acknowledged receipt of documents
- Maintaining audit trails
- Integrating with your most valued business applications and enterprise systems

Adobe Sign supports both e-signatures and [digital signatures](#). E-signatures are a way to indicate consent or approval on digital documents and forms. E-signatures are legally valid and enforceable in many industrialized nations around the world. A digital signature, by contrast, is a specific implementation of an e-signature that uses a certificate-based digital ID to verify signer identity and binds the signature to the document with encryption. Adobe Sign works with digital IDs stored on smart cards, USB tokens, and cloud-based hardware security modules (HSMs). And it supports open, standards-based signing with digital IDs across desktop, web, and mobile using the Cloud Signature Consortium specification.

This paper provides a high-level overview of Adobe Sign architecture, security, compliance, identity management, document handling, network protection, performance monitoring, service management, governance, and other key technical topics. For additional information on using differing signature types, see the Adobe [Transform business processes with electronic and digital signature solutions](#) white paper.

Architecture

The Adobe Sign architecture is designed to scale and handle large volumes of transactions without performance degradation. To provide a high level of availability and scalability, all Adobe Sign transactional data is stored in multiple distributed redundant database clusters with automatic failover and recovery.¹ The following layered architectural diagram depicts the logical division of Adobe Sign components and functionality:



Adobe Sign high-level logical architecture

Each logical layer in the Adobe Sign application is monitored by an extensive suite of tools that keeps track of key indicators, such as average time to convert documents into PDFs or resource usage. The monitoring dashboard allows Adobe Sign operations engineers to easily view the overall health of the service. Real-time notifications alert operations engineers if any of the key indicators fall outside of their defined monitoring thresholds. If an issue can't be averted, Adobe Sign keeps extensive diagnostic and forensic logs to help engineers resolve the issue quickly and address the root cause to avoid a potential recurrence.

Presentation layer

The presentation layer manages the web user interface (UI) as well as the generation, display, and rendering of documents for signature, final certified PDF files, and workflow components.

Services layer

The services layer handles the required controlling functions for the client services and web services API interfaces, such as the REST Gateway and SOAP API. The external-facing systems web servers handle browser and API requests, and the email servers manage inbound and outbound communications traffic. The web servers distribute complex dynamic requests to the Adobe Sign application servers in the business layer through the use of load balancers. The services layer web servers also incorporate security filtering rules to prevent common web attacks and firewall protection to strengthen access control.

¹ Automatic recovery is limited to Amazon Web Services infrastructure.

Business layer

The Adobe Sign business layer handles the workflow, capability-based security, document conversion and imaging services, event management, logging and monitoring, file access and manipulation, and communications functions.

Workflow engine

The Adobe Sign workflow engine executes and manages all the business processes and steps that a document needs throughout the signature process. The workflow engine uses a declarative XML-based definition language to describe the preconditions for executing customer-specific flows and the sequence of events required to complete a signature or approval process.

Capability-based security

The Adobe Sign capability-based security defines, controls, and audits which resources are available and what operations are allowed by an authenticated user or application on those resources. Resources include any information in the form of documents, data, metadata, user information, reports, and APIs.

Event management

Adobe Sign event management records and preserves an audit trail for relevant information pertaining to each user and document at each step in the workflow process. As each stage in the workflow occurs, Adobe Sign generates an event and distributes messaging via an asynchronous messaging system to the appropriate system resources.

Communications

Adobe Sign uses email for signature event notifications and optional delivery of signed and certified documents at the end of the process. To minimize spam and phishing, Adobe Sign enables authenticated email with Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), and Sender Policy Framework (SPF).

Document processing and access

To increase performance, the Adobe Sign document-processing engine provides completely stateless functionality for converting different file formats into PDF, encrypting and decrypting files, and rasterizing images for viewing through a web browser. For document processing actions, Adobe Sign relies on an asynchronous, queue-based messaging system to communicate across system resources. Additionally, all document processing and access to network-attached storage (NAS) occurs in the background, allowing Adobe Sign processing to appear instantaneous for users at each step in the workflow.

Data layer

The data layer is responsible for transactional database access, the asynchronous messaging system database, and the document store. Transactional data stored in the data access layer includes the original customer document, intermediate document versions generated during the signature process, document metadata, users, events, and the final signed PDF document processed by Adobe Sign.

Integrations

Adobe Sign also has turnkey integrations for a wide variety of business applications and enterprise systems, including Salesforce, Apttus, Workday, and Ariba, plus Microsoft solutions such as SharePoint, Dynamics, and Office applications. Additionally, Adobe Sign exposes a comprehensive set of APIs that allow for custom integration with proprietary business systems or company websites via secure HTTPS, SOAP, or REST web services. To view the list of integrations supported by Adobe Sign, see the [integrations overview page](#).

Identity management

Adobe Sign uses a role-based model for identity management that handles authentication, authorization, and access control throughout the Adobe Sign system. Capability-based security and authentication processes are defined and enabled for an organization by an Adobe Sign administrator. Adobe Sign defines general user roles for:

- **Sender**—Licensed user granted specific Adobe Sign permissions by an administrator to create document-signing workflows and send documents for signature, approval, or viewing.
- **Signer**—Verified user provided access by a sender to sign a specific document. By default, Adobe Sign sends an email to the signer that includes a unique URL to the document to be signed that is comprised of exclusive identifiers that are specific to the transaction.
- **Approver**—Verified user provided access by a sender to approve a document.
- **Other**—Verified user provided specific access by a sender to view a document or audit trail.

User authentication

Adobe Sign supports multiple methods to authenticate a user's identity, including both single factor and multifactor authentication, plus additional options to verify a user's identity. Typically, a licensed user will log in to Adobe Sign using a verified email address and password that maps to an authenticated identity, such as an Adobe ID. Administrators may also choose to configure password strength and complexity, frequency of change, past password comparison, and lockout policies (such as login renewal expiration).

Basic authentication to Adobe Sign is achieved by sending an email request to a specific person. Because most users have unique access to one email account, this is considered the first level of authentication. First level of authentication is often used for signer, approver, or other user types. To improve security and help prevent malicious individuals from spoofing the system, multifactor authentication methods such as telephone, SMS text, or knowledge-based authentication (KBA) can also be added depending on availability in your geographical location.

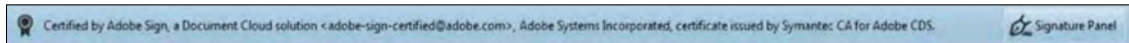
Adobe Sign supports the following types of user authentication options:

- **Adobe Sign ID**—A verified email address and password combination that is used by a licensed user to securely log in to an Adobe Sign account.
- **Adobe ID**—An Adobe ID may be used to access all licensed Adobe services, including Adobe Sign. Adobe continually monitors all Adobe ID accounts for unusual or anomalous activity to quickly mitigate any potential security threats.
- **Google ID**—User identification authenticated by Google, such as Gmail or G Suite.
- **Single sign-on (SSO)**—Enterprises seeking a tighter access control mechanism can enable Security Assertion Markup Language (SAML) SSO to manage Adobe Sign users through their corporate identity system. Adobe Sign can also be configured to recognize and integrate with leading identity management vendors, including Okta and OneLogin.

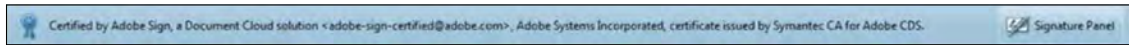
Document certification

At each stage in the workflow, Adobe Sign maintains a secure checksum of the document to help ensure both document integrity and confidentiality. Adobe Sign uses public key infrastructure (PKI) to certify final signed PDF documents with a digital signature before distributing to all participants.

The digital signature is created with a hashing algorithm that takes specific unique information in the final signed PDF to output a fixed-length, cryptographically sound, hex-encoded string of numbers and letters. Displayed graphically as the blue banner and certification badge at the top of the final signed PDF, the digital signature verifies document integrity (see the following figure) and provides assurance that the document has not been tampered with since the certificate was applied. The final certified PDF can also be further secured with a password as needed.



Acrobat DC version—black badge



Acrobat X and XI—blue badge (versions 10 and 11)

Adobe Sign document certification banners and badges

To generate the keys used to lock and certify the final signed PDF, Adobe Sign uses specific certificates issued by trusted certificate authorities (CAs) and timestamp authorities (TSAs). In certain circumstances, Adobe Sign can be configured to issue certified documents using government-required CAs, such as in Switzerland, Brazil, and India. PKI keys used to certify the final PDF are stored in a hardware security module to prevent online attacks and tampering.

Security

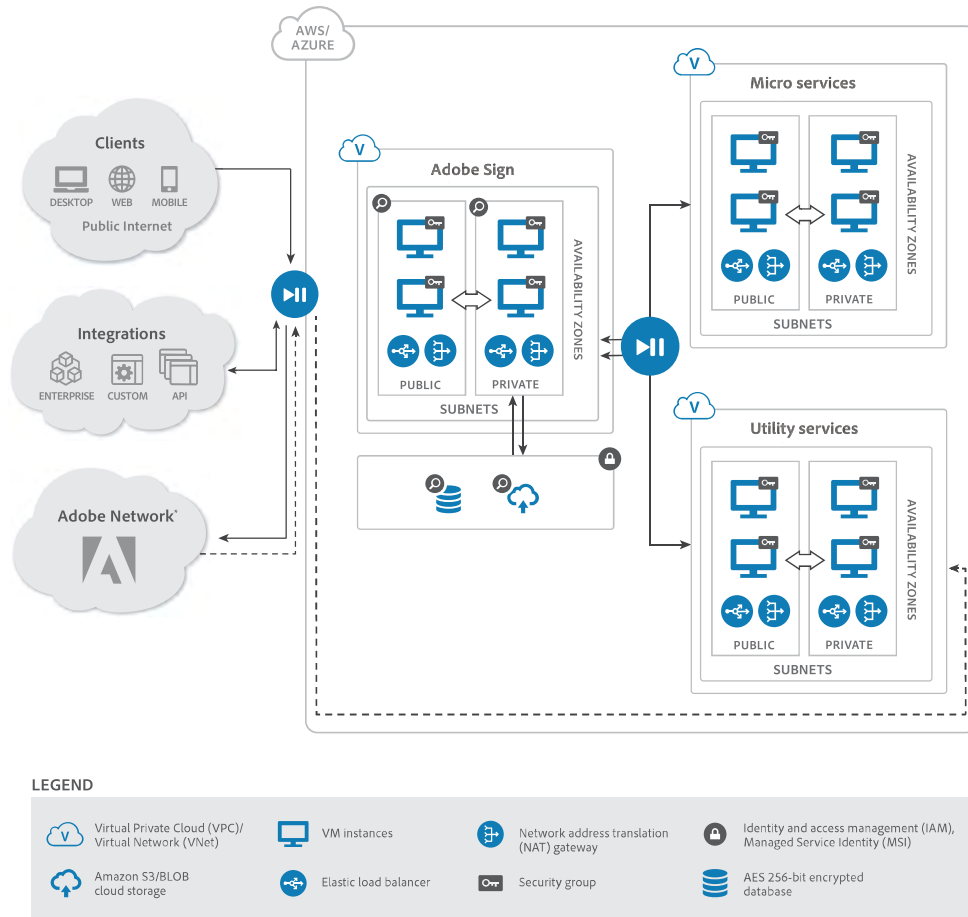
At Adobe, security and privacy practices are deeply ingrained into our culture and software development, as well as our service operations processes. Adobe Sign employs industry-standard security practices—for identity management, data confidentiality, and document integrity—to help protect your documents, data, and personal information. The Adobe Sign service infrastructure resides in American National Standards Institute (ANSI) tier 4 data centers managed by our trusted cloud service providers, Amazon Web Services (AWS) and Microsoft Azure.² All Adobe Sign infrastructure hosting partners maintain very strict controls around data center access, fault tolerance, environmental controls, and network security. Only approved, authorized Adobe employees, cloud service provider employees and contractors with a legitimate, documented business are allowed access to the secured sites in North America, Japan, Australia, India, and the EU.

As part of our commitment to security, Adobe reviews compliance attestations, such as SOC 2–Type 2 and ISO 27001 reports, on a regular basis and actively monitors all Adobe Sign components using industry-standard intrusion detection systems (IDS) and intrusion prevention systems (IPS). For additional information about Adobe security processes, community engagement, and the Adobe Secure Product Lifecycle, see www.adobe.com/security.

² Planned availability in Q3 2018.

Network security architecture

The following high-level network diagram depicts Adobe Sign security architecture including external-facing servers, cloud servers, and client access:



External-facing servers

The external-facing systems within the hosted network architecture of Adobe Sign services include *web servers* to handle browser and API requests, and *email servers* that handle inbound and outbound email traffic. Leveraging hardware load balancers, the web servers are responsible for distributing complex dynamic requests into the application servers. The web servers include built-in security filtering rules to deny common web attacks and firewall protection to help ensure strong access control.

Virtualized cloud networks

The Adobe Sign network security architecture also relies on several virtualized cloud networks. In the AWS environment these are referred to as a Virtual Private Cloud (VPC), and Microsoft Azure uses the term Virtual Network (VNet). A VPC/VNet is a logically isolated network separated and inaccessible from other instances of Adobe Sign. Within each VPC/VNet there are subnets, which contain a range of IP addresses. Subnets may be either public or private. A public subnet is connected to the Internet; a private subnet is not connected to the Internet. VPC/VNets used by the Adobe Sign service include:

- Adobe Sign private and public VPC/VNet networks are responsible for the Adobe Sign service business processes. The Adobe Sign business logic is managed in a private subnet running on scalable, secure, virtual cloud servers that are only accessible via connections originating from the public subnet.
- Microservices VPC/VNets rely on a compartmentalized container architecture to allow for highly scalable and performant "contained" services that do not impact the underlying system infrastructure. Adobe Sign

uses microservices for specific actions such as digital signature integration with the Cloud Signature Consortium, signature validation, and background removal of signature images.

- Utility services VPC/VNets manage event monitoring and logging as well as service artifact replication repositories.

From a network architecture perspective, an availability zone (AZ) lives within the VPC/VNet instance. Physically, each AZ has multiple, different redundant data centers. All data is replicated across all data centers, and across multiple servers within each data center.

VPC/VNet instances are locked down to a security group. Similar to a virtual firewall, the security groups allow Adobe to further control inbound and outbound traffic to the VPC/VNet instance. This allows Adobe to make sure that only validated users are performing authorized actions. Additionally, the Adobe Sign network security architecture includes intrusion detection/protection sensors at key locations to help ensure system integrity and visibility across the service.

Client access

The Adobe Sign service is accessible from a variety of client endpoints, such as a browser, mobile app, or via email. When a client connects to Adobe Sign in its assigned region, it connects through an Internet gateway to several VPC/VNets. All the client connections occur over a HTTPS connection utilizing TLS1.2 (as of June 2018) with a minimum of AES 128-bit encryption.

Network protection

All Adobe Sign service providers employ network devices to monitor and control communications at the external boundary of the network as well as key internal boundaries within the network. These firewall and other boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to control and enforce the flow of traffic and are kept up to date by automated processes.

Both providers also employ a variety of automated monitoring systems to help ensure a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities and conditions at network ingress and egress points to protect against traditional network security vulnerabilities such as:

- Distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MITM) attacks
- Internet protocol (IP) spoofing
- Port scanning
- Packet sniffing by other tenants

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) to establish secure connections to manage the hosted infrastructure for Document Cloud services.

Encryption

Adobe Sign only employs *PCI DSS approved encryption algorithms* to encrypt documents and assets at rest with AES 256-bit encryption, and supports HTTPS TLS v1.2 (plus other legacy versions) to help ensure that data in transit is also protected. Documents at rest are secured in encrypted storage containers which are only accessible with the appropriate capability-based security permissions through the application data access layer in a private subnet. Additionally, Adobe Sign senders also have the option to further secure a document with a private password.

Document encryption keys are stored in a secure environment with restricted access and are rotated as necessary in accordance with the Adobe Key Management Standard. Each trusted hosting provider employs strong multifactor encryption, such as encrypting each object with a unique key and, as an additional safeguard, encrypting the key itself with a master key that it regularly rotates.

Compliance

As a global e-signature solution designed for verified signers to interact with digital documents from any location or any device, Adobe Sign meets or can be configured to meet compliance requirements for many industry and regulatory standards. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU. For more information on Adobe privacy policies, please see www.adobe.com/privacy, and to learn more about e-signature laws in a specific region, see the [Global Guide to Electronic Signature Law: Country by country summaries of law and enforceability](#).

ISO 27001

The ISO 27001 standard is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It contains requirements for information security management systems (ISMS) that can be audited by an independent and accredited certification authority. Adobe Sign is ISO 27001: 2013 certified.

SOC

The Service Organization Controls (SOC) is a series of IT controls for security, availability, processing integrity, confidentiality, and privacy (Type 2). Adobe Sign is SOC 2-Type 2 (Security & Availability) certified.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes to increase controls around cardholder data management and reduce fraud. As part of Adobe Document Cloud, Adobe Sign has achieved attestation for PCI DSS compliance as a merchant and service provider.

FedRAMP

The U.S. Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud products and services used by government agencies. FedRAMP Tailored is a baseline for cloud service providers with Low-Impact Software-as-a-Service (LI-SaaS) Systems. Adobe Sign is FedRAMP Tailored certified.

SAFE-BioPharma

The SAFE-BioPharma® digital identification and digital signature standard was created by the biopharmaceutical industry and its regulators to provide global high-assurance identity trust for cyber transactions in biopharmaceuticals, biotech, and healthcare industries. Adobe Sign is SAFE-BioPharma certified.

HIPAA³

The Health Insurance Portability and Accountability Act (HIPAA) helps ensure sensitive patient information is protected by establishing standards for electronic healthcare transactions. Adobe Sign is ready to support HIPAA compliance for any organization that meets the definition of a covered entity as outlined by the U.S. Department of Health and Human Services (HHS) and signs a business associate agreement (BAA) with Adobe.

21 CFR Part 11³

The Code of Federal Regulations, Title 21, Part 11: Electronic Records; Electronic Signatures (21 CFR Part 11) establishes the U.S. Food and Drug Administration (FDA) regulations on electronic records and electronic signatures.

GLBA³

The U.S. Gramm-Leach-Bliley Act (GLBA) provides regulations for financial institutions that help ensure the privacy of personal customer information. Adobe Sign is ready to comply with GLBA.

³ An Adobe service that is GLBA-ready, FERPA-ready, FDA 21 CFR Part 11 compliant, or HIPAA compliant means that the service can be used in a way that enables the customer to help meet its legal obligations related to the use of service providers. Ultimately, the customer is responsible for ensuring compliance with legal obligations, that the Adobe service meets its compliance needs, and that the customer secures the service appropriately.

FERPA³

The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. student education records and directory information. Under FERPA guidelines, Adobe Sign is ready to contractually agree to act as a "school official" when handling regulated student data to enable our education customers to comply with FERPA requirements.

Operations

Adobe employs standard operations practices, such as performance monitoring to manage the health of the Adobe Sign service.

Performance monitoring

Adobe conducts extensive monitoring activities to help ensure the health of the Adobe Sign service, including availability, volume, and performance checks. All health checks are based on defined and measurable thresholds that are preemptive indicators of a need for preventative measures. Health-check thresholds and processes are reviewed on a regular basis.

Adobe also conducts server-side logging of customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs do not store any personally identifiable information (PII), such as passwords or names, except for the Adobe ID if applicable. Only authorized Adobe technical support personnel, key engineers, and select developers have access to the logs to diagnose specific issues that may arise.

Service management

Adobe leverages industry-standard service management concepts such as change, incident, and problem management. Our processes and controls are also designed to support numerous compliance frameworks.

Change management

Adobe enforces a comprehensive, standards-compliant change management process with rigorous inspections to assess potential impacts and benefits for any changes to the Adobe Sign service. Most changes have no impact on the service. However, there are rare exceptions, such as the annual disaster-recovery procedures test that may impact the customer experience. In such special cases, Adobe will provide advance notification to any potentially impacted Adobe Sign customers.

Incident management

In the case of a service disruption, the Adobe Sign operations team will invoke Adobe's incident management process. When this process is invoked, 24x7x365 on-call engineers are brought together via online collaboration tools to triage, solve, and resolve the issue. The incident management process also has provisions to capture data on the chain of events leading to the incident resolution, as well as timing and impact information used to assess the impact to our service level agreements (SLAs). Any outstanding issues are transitioned to the problem-management team for ongoing governance.

Problem management

As part of the Adobe incident management process, a formal post-mortem problem-management meeting is scheduled to review the root cause of the incident and propose preventive actions. Since other incidental discoveries may occur during outages, the problem-management process is used to address these along with any vulnerabilities that have either contributed to an outage or have a high risk of causing an outage in the future. The output of a problem-management process is an analysis and summary of the incident, a detailed explanation of the root cause, impact analysis, and required corrective actions to help ensure that the problem is fully resolved.

Staffing

Adobe maintains a dedicated, geographically dispersed team of technical operations engineers who use a "follow-the-sun" model where working hours are allocated during regular business hours. This global team provides 24x7x365 on-call response support to assist the corporate Adobe incident response team with resolving any disruption to the service as quickly as possible. Most of Adobe's on-call technical operations engineers are located in the United States and Noida, India.

Governance

Whether monitoring for new vulnerabilities or mitigating potential threats, Adobe employs industry-standard practices to help ensure the Adobe Sign risk management, mitigation, and incident resolution process is agile and thorough.

Risk management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. Adobe continuously monitors the threat landscape, shares its knowledge with security experts around the world, and endeavors to swiftly resolve incidents. All Adobe Sign infrastructure providers use several tools to proactively detect, evaluate, and trace network-wide traffic and other potentially threatening anomalies, such as denial-of-service (DoS) attacks.

Penetration testing

Adobe approves and engages with third-party security firms to perform penetration testing designed to uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe will document these vulnerabilities, evaluate severity and priority, and then create a mitigation strategy or remediation plan for the Adobe Sign service.

Prior to each release, the Adobe Sign security team performs a risk assessment of the service to look for insecure network setup issues across firewalls, load balancers, and server hardware, as well as application-level vulnerabilities. The risk assessment is conducted by highly trained security staff trusted with securing the network topology and infrastructure, as well as the Adobe Sign service. The security touchpoints include threat modeling exercises along with vulnerability scanning and static/dynamic analysis of the application.

Threat mitigation

To mitigate new vulnerabilities and threats that evolve on a daily basis, Adobe subscribes to industry-wide vulnerability announcement lists, such as US-CERT, Bugtraq, and SANS, as well as security alert lists issued by major security vendors. For cloud-based services, such as Adobe Sign, Adobe centralizes incident response, decision-making, and external monitoring to provide cross-functional consistency and fast resolution of issues.

If a significant vulnerability is announced that puts Adobe Sign at risk, the vulnerability is communicated to the appropriate teams within the Adobe Document Cloud organization to coordinate the mitigation effort. Additionally, if an incident occurs with the Adobe Sign service, incident response and development teams use industry-standard practices to identify, mitigate, and resolve the incident:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

To assist with forensic analysis of an incident, the Adobe Sign team captures a complete image (or memory dump) of an impacted machine(s), evidence safe holding, and chain-of-custody recording.

Disaster recovery

Adobe Sign data centers are highly resilient, designed to deliver high availability and tolerate system or hardware failures with minimal impact. To help ensure business continuity, Adobe maintains regional disaster recovery plans for Adobe Sign when hosted on AWS infrastructure in the U.S. and EU along with documentation in the form of an annual run book that outlines all the steps required to complete a data center failover. Additionally, Adobe strives to achieve the following disaster recovery parameters for its Adobe Sign customers:

- **Recovery point objective (RPO)**—Refers to the amount of data that could potentially be lost during disaster recovery. The timeframe is determined by the amount of time between data protection events. The RPO for Adobe Sign is 2 hours.
- **Recovery time objective (RTO)**—Relates to potential downtime. The metric refers to the amount of time it could take to recover from a data-loss event and how long it takes to return to service. The RTO for Adobe Sign is 8 hours.

Customer notification

Adobe Sign uptime data is available at www.adobe.com/go/trust-dc. Additionally, for both planned and unplanned system downtime, Adobe Sign also follows a notification process to inform customers about the status of the service.

If there is a need to migrate the operational service from a primary site to a disaster-recovery site, customers will receive several specific notifications including:

- Notification of the intent to migrate the services to the disaster-recovery site
- Hourly progress updates during the service migration
- Notification of completion of the migration to the disaster-recovery site

The notifications will also include contact information and availability for client support and customer success representatives. These representatives will answer questions and concerns during the migration as well as after the migration to promote a seamless transition to newly active operations on a different regional site.

Data isolation/segregation

All cloud services partners use strong tenant isolation security and control capabilities to segregate Adobe Sign customer data within the multitenant service. Security management processes and other security controls are also used to help ensure that customer data is appropriately isolated and protected.

For more information

Solution details: www.adobe.com/go/adobesign

Electronic signature legality:

<https://acrobat.adobe.com/us/en/sign/capabilities/electronic-signature-legality.html>

Adobe security: www.adobe.com/security

Adobe Trust Center: www.adobe.com/trust.html

Microsoft Azure security: azure.microsoft.com/services/security-center

Amazon Web Services security: <https://aws.amazon.com/security>

Adobe Sign Help/Enabling Single Sign-On with SAML:

https://helpx.adobe.com/sign/help/SAML_Configuration.html



[Sign In](#)**SIGN** ▾

Archiving agreements externally



Search

Set up your external archive

Archive copies of signed agreements to any email address or to Box and Evernote. A copy of the Signed and Filed email is sent to either the email address you provide or to the service you set up.

Archives are perfect for keeping backup copies of the agreements you've sent.

Applies to: **Sign**Last Published: **August 27, 2017**

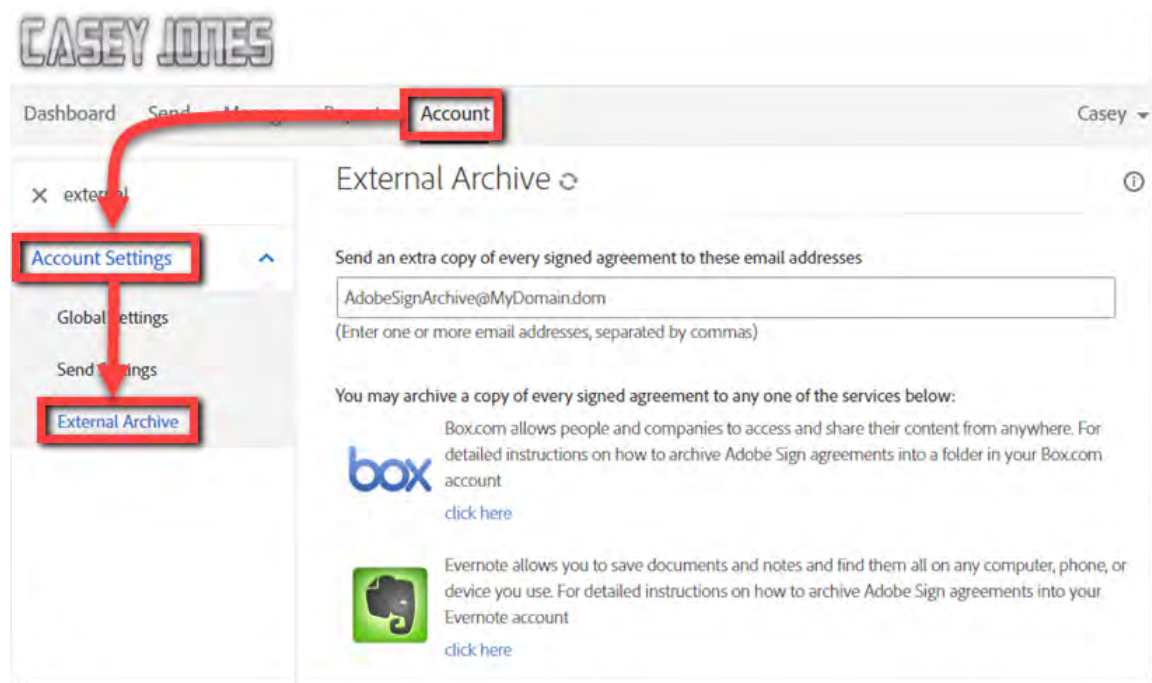
External archive: Email address

▼ Quick steps

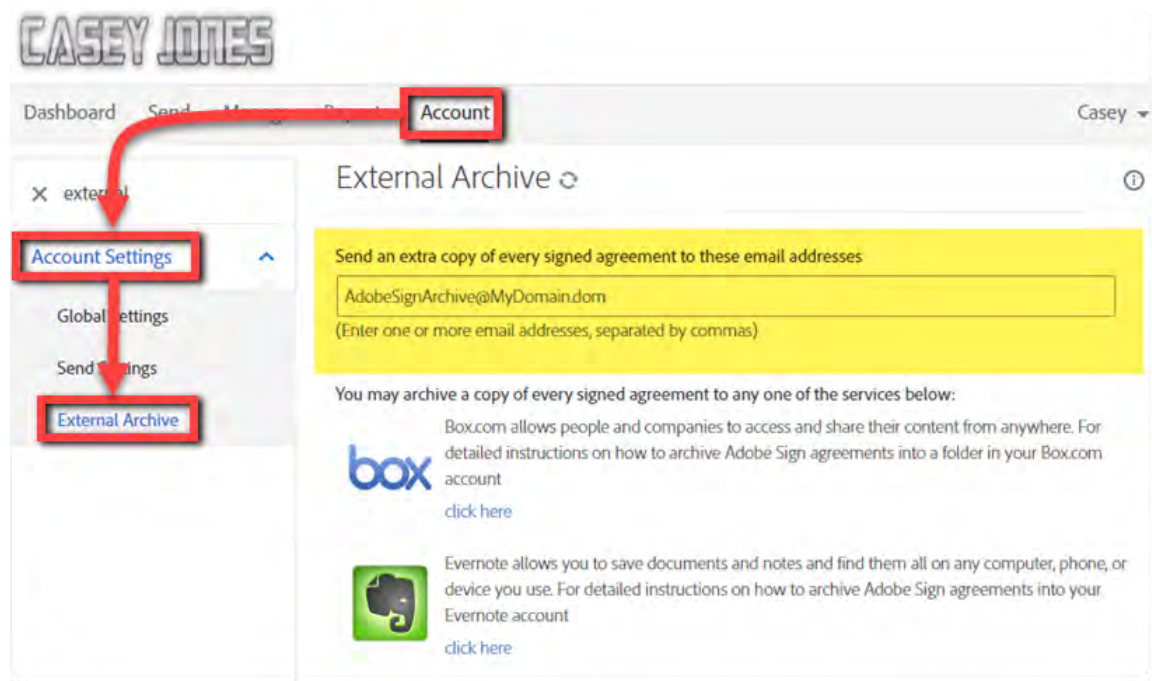
1. As account admin, go to the **Account** page.
2. Click **Account Settings**.
3. Click **External Archive**.
4. Enter the alternate email address you want the copies sent to.
5. Click **Save Changes**.

▼ Step-by-step

- 1 Log in as the account admin, go to the **Account** tab, and click **Account Settings** and **External Archive**.



- 2 Enter the email address that you want to use as your archive and click **Save Changes**.



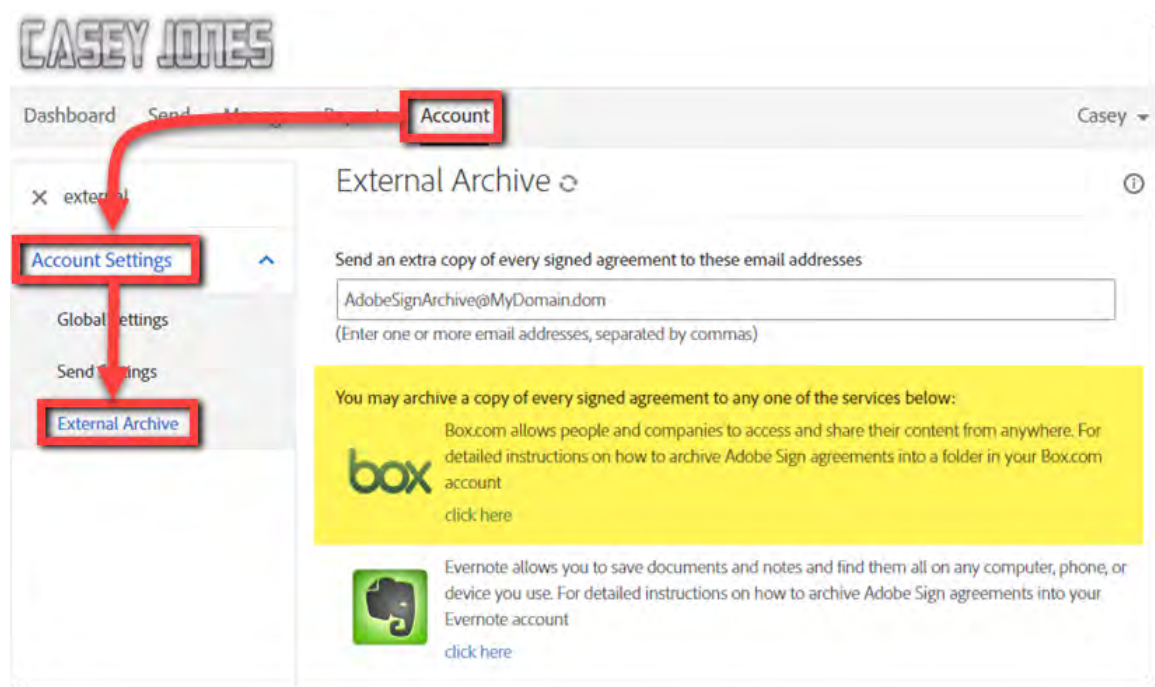
External archive: Box.com

Quick steps

1. As account admin, go to the **Account** page.
2. Click **Account Settings**.
3. Click **External Archive**.
4. Click the **click here** link next to the Box logo.
5. Follow the instructions in the pop-up window.

Step-by-step

- 1 To set up your External Archive with your Box account, log in as the Account Admin and go to the **Account** tab. Click **Account Settings**, **External Archive** and then click the **click here** link to the right of the Box logo.



- 2 Follow the Box-specific directions in the pop-up window.

Archive Your E-signed Adobe Document Cloud Contracts in Box.com

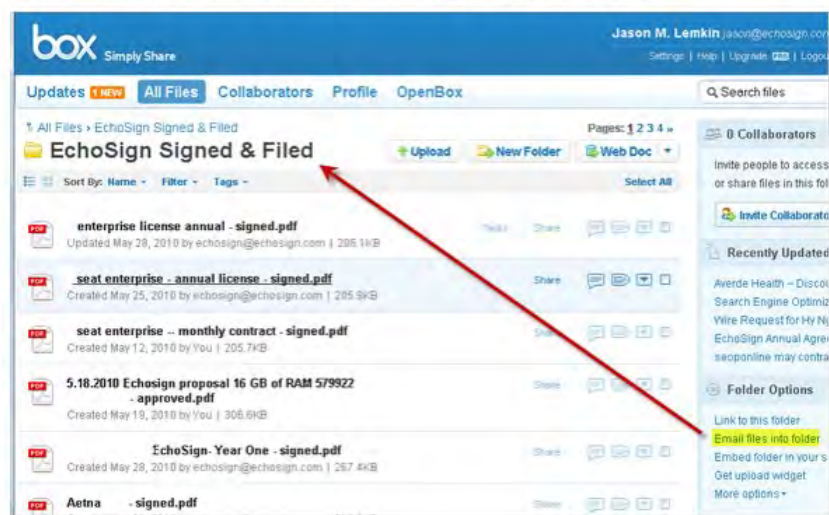
Box.com, which has had native [integration](#) of Adobe Document Cloud via its OpenBox platform since 2007, has recently added a great feature which enables all your signed contracts to be stored not only on Adobe Document Cloud but in Box.com as well – via [Box Folder Email Addresses](#).

To archive your Adobe Document Cloud contracts in Box.com follow the steps below:

- 1 In Box.com, create a folder for your signed contracts – e.g. “Adobe Document Cloud Signed & Filed”.
- 2 Click “Email files into folder” and copy the email address appearing in the pop-up window.
- 3 Paste this email address in the “External Archive” Settings in your Adobe Document Cloud account.
- 4 >Click “Save Changes”.

From now on, all your signed contracts will be stored not only on your Adobe Document Cloud Manage tab (and/or in Salesforce.com, etc.), but inside of Box.com too.

You may then share access to that Box.com folder with other users in your organization who need access to copies of all signed agreements (e.g., legal, finance, sales).



You can of course also send contracts for e-signature from Box.com as well, using Adobe Document Cloud for OpenBox. This allows you to send documents for signature from within Box.com and automatically get all signed copies back into Box.

To learn more about Adobe Document Cloud for Box.com, click [here](#).

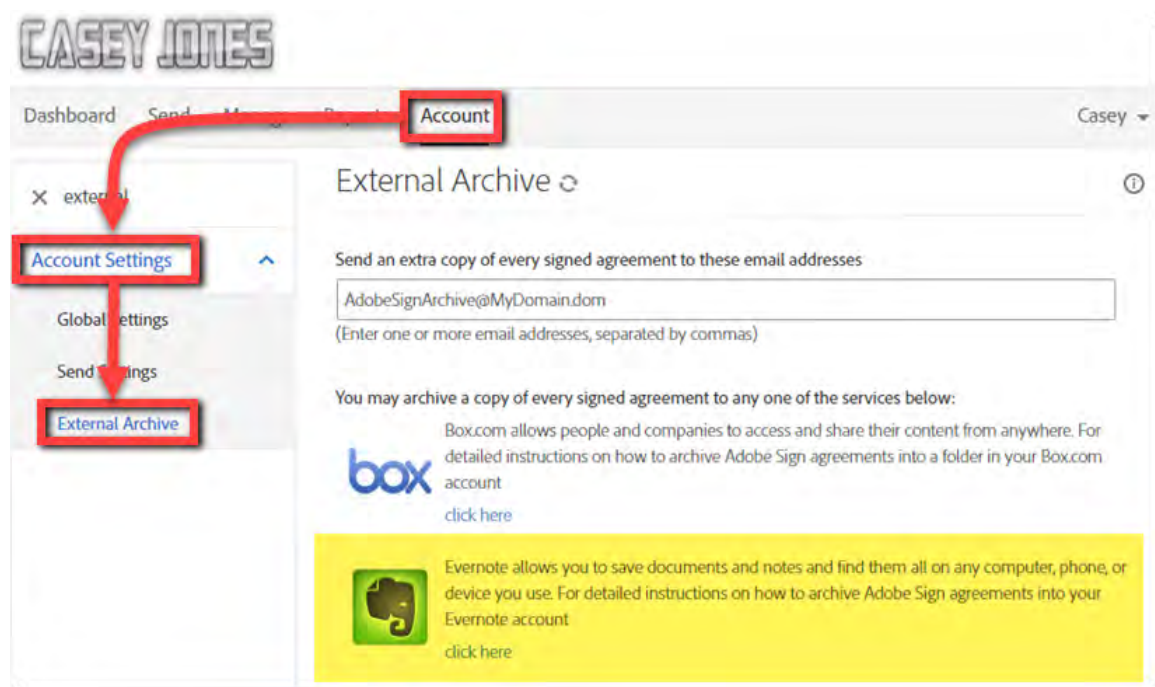
External archive: Evernote

Quick steps

1. As account admin, go to the **Account** page.
2. Click **Account Settings**.
3. Click **External Archive**.
4. Click the **click here** link next to the Evernote logo.
5. Follow the instructions in the pop-up window.

Step-by-step

- 1 To link your Evernote account to your External Archive, log in as the Account Admin and go to the **Account** page. Click **Account Settings**, **External Archive** and click the **click here** link to the right of the Evernote logo.



- 2 Follow the Evernote specific directions in the pop-up window.

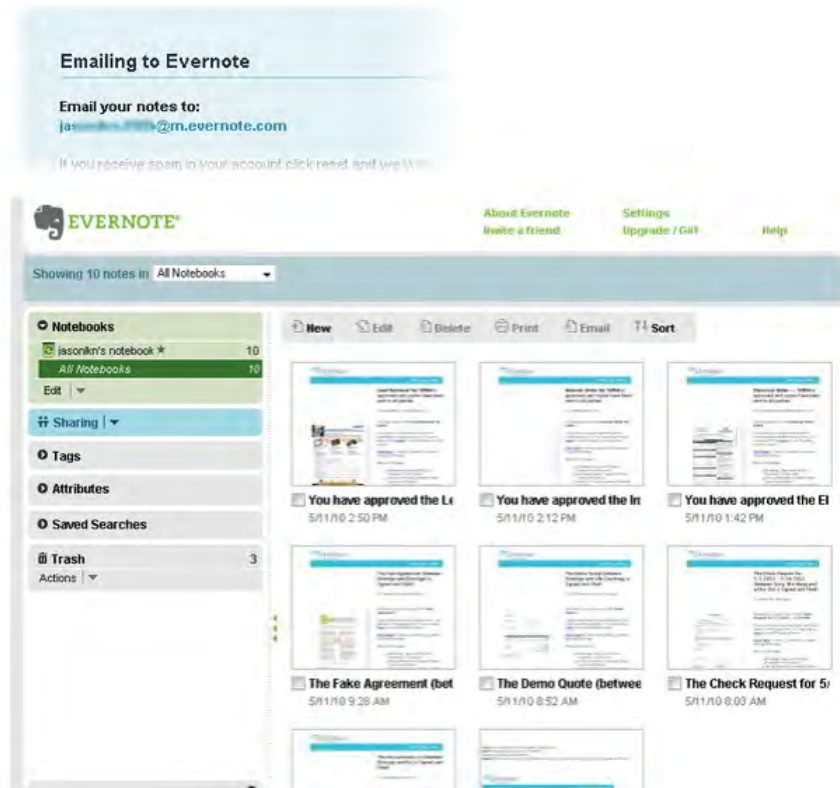
Archive Your E-signed Adobe Document Cloud Contracts in Evernote

Evernote is an extremely popular service that lets you very easily store your notes, emails, PDFs, photos, etc. all in one central place that is nicely indexed and searchable. And now you can now archive all your signed contracts to be stored not only on Adobe Document Cloud but in Evernote as well.

To archive your Adobe Document Cloud contracts in Evernote follow the steps below:

- 1 In Evernote's Settings page, look for the "Emailing to Evernote" section.
- 2 Copy the email address appearing under "Email your notes to:".
- 3 Paste this email address in the "External Archive" Settings in your Adobe Document Cloud account.
- 4 Click "Save Changes".

From now on, all your signed contracts will be stored not only on your Adobe Document Cloud Manage tab (and/or in Salesforce.com, etc.), but in Evernote too.





Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

[Sign In](#)**SIGN** ▾

How to archive a document in Adobe Sign

Search Adobe Support

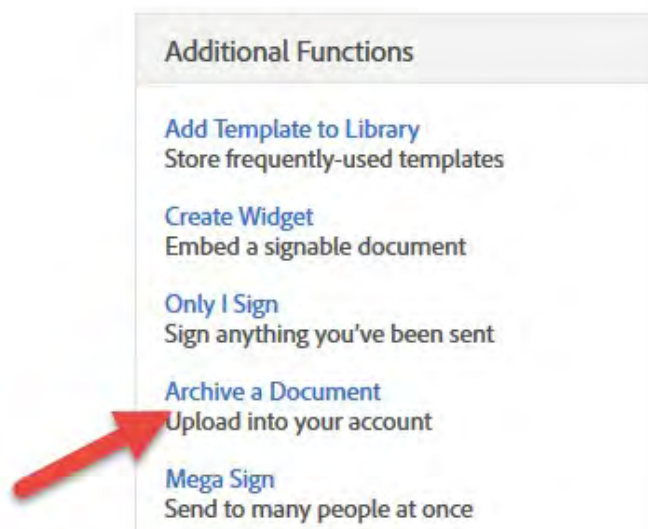
You can archive documents to store them securely.

Search

Applies to: **Sign**

Last Published: **October 4, 2017**

- 1 **Log in** to your Adobe Sign account.
- 2 Click the **Dashboard** tab.
- 3 Under the Additional Functions section, click **Archive a Document**.



- 4 The below screen appears.

The screenshot shows the Adobe Sign interface for archiving a document. At the top, there is a navigation bar with the Adobe Sign logo and links to Dashboard, Send, Manage, Reports, and Account. Below this is the title 'Archive a Document' with a note that bold fields are required. The form contains several input fields: 'Document Name' (required), 'Party's First Name', 'Party's Last Name', 'Company', 'Date' (pre-filled with 02/15/2017 and a calendar icon), and a 'Message' text area. At the bottom of the form is a 'Document' section with a 'Browse...' button and the text 'No file selected'. Below the form is a section to 'also send a copy of this document to' with an email address input field. A blue 'Archive' button is located at the bottom right of the form.

Adobe Sign

Dashboard Send Manage Reports Account

Archive a Document (Bold fields are required)

Document Name:

Party's First Name:

Party's Last Name:

Company:

Date: 02/15/2017

Message:

Document: No file selected

...also send a copy of this document to:

- 5 You can then name the document that you want to archive (Fields marked in bold are required).
- 6 Click Browse to select the file that you want to archive.
- 7 Once you have selected the document, click Archive.
- 8 The document then appears in the Archived section on the Manage tab in your Adobe Sign account.

Additional information

Please note that the document can only be archived one at a time and only from the local system so you have to ensure that it is already saved on your computer.



Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

[Sign In](#)

SIGN ▾

Multilanguage sending and signing



Search

Set up multilanguage sending and signing

All Adobe Sign plans let both senders and signers select their choice from 34 available languages, including English, German, Chinese, Japanese, Korean, French, Spanish, Italian, Dutch, and more. The enterprise plan also lets senders request signatures in any language.

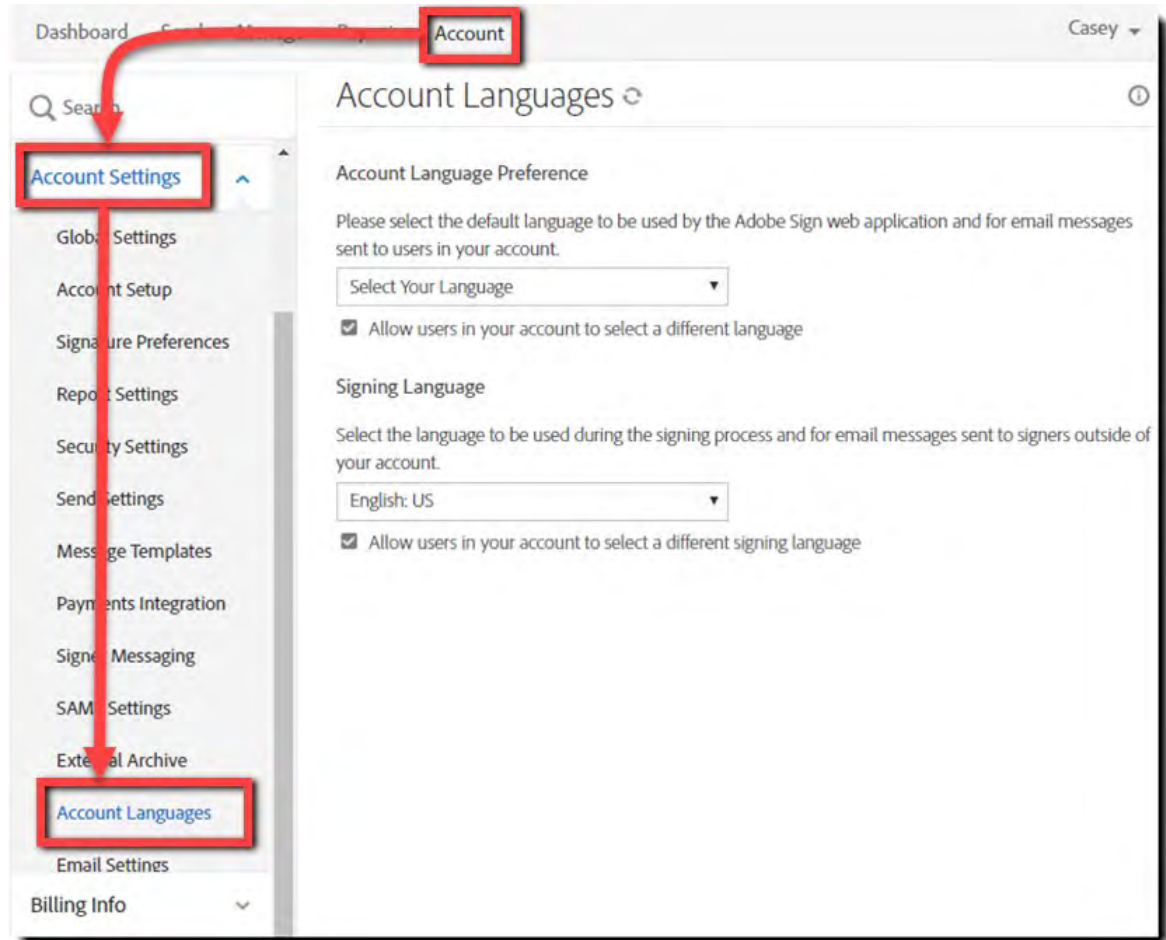
Applies to: **Sign**Last Published: **November 29, 2017**

▼ Quick steps

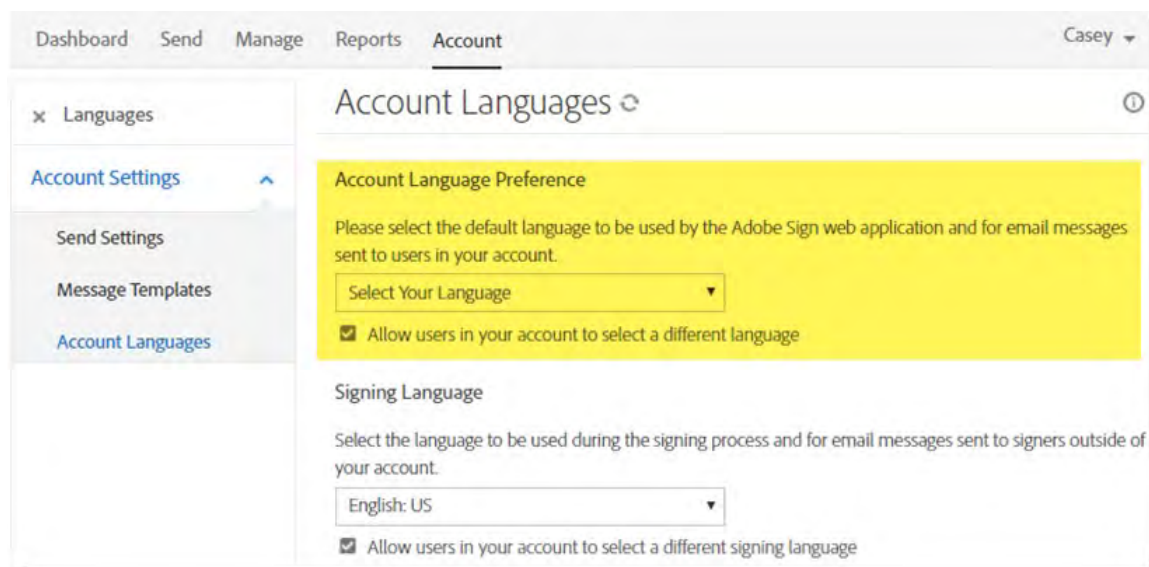
1. As account admin, go to the **Account** page.
2. Click **Account Languages**.
3. Choose the default Adobe Sign web application language or signing experience language.
4. Check if you want users or signers to have the option to set the language themselves.
5. Click **Save Changes**.

▼ Step-by-step

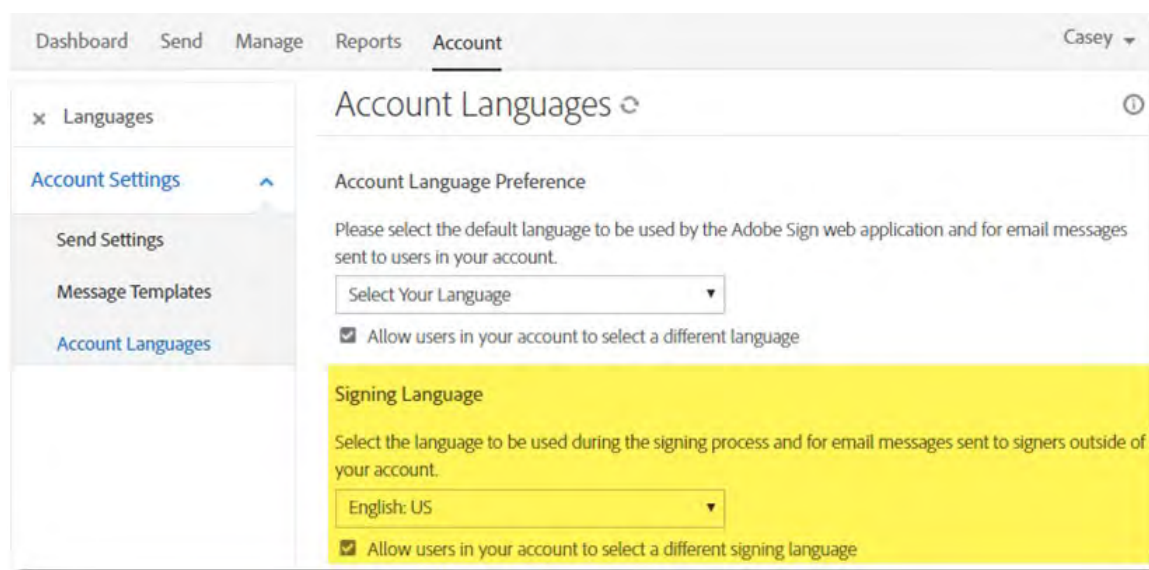
- 1 As account admin, got to the **Account** page and click **Account Languages**.




- 2 To change the default language of the web application, for users in your account, select a language from the drop-down list under **Account Language Preference**. You can also either allow or deny users access to change the language by selecting this option.



- 3 To change the language of the signing experience for your signers, select the desired language from the drop-down list under **Signing Language**. You can allow or deny signers the ability to change the language of the signing experience by selecting this option.



 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)

**SIGN**[^ Back to top](#)[< See all apps](#)[Learn & Support](#)[Get Started](#)[User Guide](#)[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region 

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)



**Add e-signature and PDF
workflows to your existing
systems.**

It's easy with Adobe Document Cloud
integrations.

Adobe Sign is now Microsoft's preferred e-signature solution.

[Learn more](#)

We partner with leading companies — so you can
add Adobe Document Cloud solutions to the
systems, processes, and applications your
organization already uses.

[See all integrations](#) | [See all use cases](#)



Increase workforce productivity and business transactions in Microsoft Office, SharePoint, and Dynamics.



Send, sign, track, and file contracts quickly and securely anywhere in Salesforce, including on mobile.



Get offer letters, NDAs, and other HR documents signed quickly and securely using Adobe Sign in Workday.

The APTTUS logo, with the word "APTTUS" in a bold, green, sans-serif font.

Accelerate contract and quote approval cycles by adding e-signature capabilities to any agreement.

The SAP SuccessFactors logo, with "SAP" in blue and "SuccessFactors" in a lighter blue, sans-serif font.

Add trusted, legal e-signatures that speed HCM workflows with Adobe Sign for SAP SuccessFactors.

The SAP Ariba logo, with "SAP Ariba" in blue and a stylized orange triangle icon to the right.

Cut document execution time by 80% when you add e-signatures, tracking, and automated reporting to your SAP Ariba workflow.



Handle all of your document needs, from storing and accessing to sending and signing.

Speed signature processes and create all-digital service workflows with the Adobe Sign for ServiceNow integration.

Connect Adobe Sign with Conga solutions and use them together to seamlessly speed contract approvals.

We make it easy to go digital.

Add Adobe Document Cloud solutions to your existing applications or business processes using our robust APIs.

[Learn more at Adobe I/O >](#)

[Get technical resources >](#)

Partner with Adobe Document Cloud.



Join the Adobe ISV Partner Program and we'll give your company the tools and resources to build and deliver solutions that integrate with Adobe Document Cloud.

[Become a partner >](#)

Get more out of your business systems.

Streamline processes and speed your business by running Adobe Document Cloud solutions inside your existing systems.

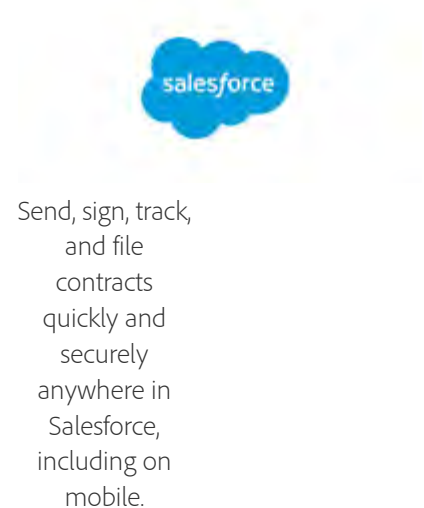
Sales/Customer Relationship Management (CRM)

Microsoft Dynamics 365

Send, sign, track, and file contracts with e-signatures you trust — anywhere, anytime, on any device — inside Microsoft Dynamics 365 CRM.



Get quotes, contracts, and agreements signed in minutes within your NetSuite account.



Send, sign, track, and file contracts quickly and securely anywhere in Salesforce, including on mobile.



Engage customers in one place across multiple channels by integrating Adobe Sign with Zoho CRM.



Close deals faster by sending contracts for e-signing from within your SugarCRM system.

Contract lifecycle management (CLM)/configure, price, quote (CPQ) software



Agiloft integrates with Adobe Sign to speed approval workflows, manage contracts, and provide full reporting and compliance.



Accelerate contract and quote approval cycles by adding e-signature capabilities to any agreement.

Streamline contract management by adding Adobe Sign to your ASC workflows.



Speed up your quoting and proposal processes with secure, automated, and trackable Adobe Sign e-signatures.



Change Healthcare uses Adobe Sign to help health plans streamline their provider contracting lifecycle.

Connect Adobe Sign with Conga solutions and use them together to seamlessly speed contract approvals.



Manage your contracts and meeting minutes more easily than ever before. Use Adobe Sign to track and store documents within ContractZen.



Speed contracting and reduce costs with e-signatures in IBM Emptoris Contract Management.



Send, sign, and track documents with Adobe Sign in concert with icertis, the leading enterprise contract management platform in the cloud.



Automate contacts and sign agreements electronically with intelligentcontract and Adobe Sign.



Speed procurement processes using Adobe Sign within Jaggaer's solutions.



Automate the creation of business-critical documents, integrated with e-signatures, for compliant processes.



Increase productivity by using Adobe Sign in Oracle's PeopleSoft applications.



Streamline lead-to-cash management with mobile contract and revenue management.



Deliver e-signatures integrated with the CPQ solution from Salesforce.



Optimize corporate contracts by improving compliance and delivering rapid time to value with SAP CLM.



Cut document execution time by 80% or more when you add e-signing, tracking, and automated reporting to your SAP Ariba workflow.



Get an end-to-end solution for complex contract automation that includes e-signatures.

Human resources (HR)/Enterprise Resource Planning (ERP)



Streamline staffing, recruiting, and payroll with Adobe Sign and Bond International Software.



COMPAS uses Adobe Sign as the fastest and easiest way to get onboarding documents signed, tracked, and filed.



Integreat HR and Adobe e-signatures help you streamline the new hire onboarding process.



Streamline hiring processes and applicant tracking that recruiters and hiring managers can focus on their candidates.



Adobe Sign integrates with Lumesse talent management software to let users send, sign, and track documents throughout the entire employment lifecycle.



Make your HR processes 100% digital with Adobe Sign and Namely.



Enable faster, paperless onboarding with Adobe Sign and Saba Recruiting@Work.



Add trusted, legal, e-signatures that speed HCM workflows with Adobe Sign and SAP SuccessFactors.



Speed signature processes and create all-digital service workflows with the Adobe Sign for ServiceNow integration.

E-signatures streamline the ability-to-pay verification process for Veri-Tax.



Get offer letters, NDAs, and other HR and finance documents signed quickly and securely using Adobe Sign with Workday.



Adobe Sign integrates with Zoho People, a complete online HR solution that centralizes and secures employee data and offers efficient self-serve features.

Collaboration Productivity



Microsoft Office 365

Create and share PDFs right in your Office 365 applications. You can also send documents for signature and track status in Word, PowerPoint, or Outlook.

Microsoft OneDrive

Get more done in OneDrive for Business online. Convert Office files to PDF and combine documents into a single file, right in OneDrive.

Microsoft SharePoint

Use Document Cloud solutions with SharePoint to streamline your document workflows. Get agreements signed instantly, and work seamlessly with PDF files.



Together, Box and Adobe handle all of your document needs, from storing and accessing to sending and signing.



Cut cost and risk. Track and verify legal document e-signatures with Adobe Sign and CaseMail Digital Postal Service.



Open, edit, sign, and store PDFs in your Dropbox account while working in Acrobat DC.



With Adobe Sign, you can send, sign, and automatically store documents — all within the Egnyte Connect user interface.



Transform routine business functions into fully automated processes with Nintex Workflow Cloud, Document Generation, and Adobe Sign.



A platform for streamlining business processes, Pulpstream integrates with Adobe Sign to simplify legal document authentication on mobile devices.



Integrate Adobe Sign with WebMerge, an online platform that lets users collect data, populate documents, and send to any contacts automatically.



Adobe Sign enables sending, signing, and tracking documents inside Zoho Docs, an online team collaboration and group knowledge sharing tool.

Solution Partners



Benefit from a relationship with this global management consulting and technology services company.



Get industry-leading audit, consulting, tax, and advisory services.



Digitally reinvent your operations for great efficiency and transform your entire enterprise.



PwC firms help organizations and individuals create the value they're looking for.

Other



Send, sign, track, and manage agreements from your Android device.



Handle all the transactions for your property using Adobe Sign with Buildium.



Cloud Lending Solutions offers loan origination software for any financial institution.



Adobe and cPaperless help accounting firms prepare, send, route, sign, and track documents.



Manage valuable signed digital documents for ultimate security and compliance.



Add the convenience of customer payments using credit cards or e-checks with this Adobe Sign integration.



E-signatures make it easy for renters to complete vacation rental agreements in HomeAway.



Adobe Sign integrated with IMM's TotaleAtlas helps streamline business processes.



InsureSign helps insurance agents engage with customers from anywhere.



Send, sign, track, and manage agreements from your iPad, iPhone, or iPod touch.



Onboard clients swiftly and easily using Adobe Sign and a streamlined workflow with IRIS CRM.



Centralize identity management and user provisioning for Adobe Document Cloud with Okta's solution.



Sign into applications including Adobe Sign with this single sign-on portal.



Enhance close rates by allowing customers to sign orders and other documents quickly, easily, and securely.



Save time and cut paperwork by using Adobe e-signatures in Reapit's Estate Agency software.



Adobe Sign makes Reesio the complete tech solution for real estate professionals.



Expedite customer interactions, onboarding, invoicing, and payments with Adobe e-signatures.



Better manage your documents by integrating e-signatures into your Ricoh solutions.



Adobe Sign helps accelerate processes associated with managing your company's risk.



E-sign real estate documents in ShortTrack's mobile transaction management platform.



ThinkSmart helps customers build custom workflows integrated with Adobe technology.




Swiftly and accurately complete more business transactions with TMS lease solutions and Adobe Sign.



Get tax returns signed and submitted quickly and securely with Adobe Sign and Xero.

Want to know more?

Whether you need  the basic information about our solutions or you'd like a customized quote for your unique environment, we're here to help you get your questions answered.

Contact us

 855-959-0100

Adobe online services are available only to users 13 and older and require agreement to additional terms and the [Adobe Privacy Policy](#). Online services are not available in all countries or languages, may require user registration, and may be discontinued or modified in whole or in part without notice. Additional fees or subscription charges may apply.

 > Adobe Document Cloud > Business

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

Adobe I/O

Adobe Sign

OVERVIEW

A Simple Workflow

Using the APIs

Terminology

GETTING STARTED

API USAGE

SCENARIOS

API Reference

Samples

Events

Developer Guides

Migrating from SOAP

Adobe Sign

Adobe Sign

Documentation

SDK

More about Adobe Sign


Home

All APIs

Console

^

overview



As a developer, you can build a variety of integrations with Adobe Sign using just the APIs. Once built, integrations allow you to start the Adobe Sign signing experience entirely from within the external application.

You can also incorporate the functionality of Adobe Sign into any external applications by embedding the Adobe Sign UI within those applications. External applications can also receive status updates in real-time for transactions initiated using Adobe Sign. These external applications can retrieve and store copies of the signed agreements.

The Adobe Sign APIs can be used to:

- Send a document for e-signature
- Create and manage agreements
- Retrieve signed documents
- Archive signed documents
- Embed a signing UI in your app
- Send reminders
- Download audit trails
- [And a lot more!](#)

See [A Simple Workflow](#).

▼

a-simple-workflow

APIS[Creative Cloud](#)[Document Cloud](#)[Experience Cloud](#)[Adobe Cloud Platform](#)**BLOGS AND COMMUNITY**[Adobe I/O Blog](#)[Adobe I/O on Twitter](#)[Adobe on GitHub](#)[PhoneGap Blog](#)[Adobe I/O on
YouTube](#)**SUPPORT**[Contact Us](#)[Adobe on StackOverflow](#)[Adobe Product Support](#)**ADOBE**[About Adobe](#)[Open Source](#)[Privacy Policy](#)[Terms of Use](#)[Cookies](#)

Copyright © 2018 Adobe Systems Incorporated. All rights reserved.



Sign In



SIGN ▾

Adobe Sign for Microsoft - Outlook Add-in

Search Adobe Support



Search

[Click here to install the add-in from the Microsoft store](#)

Overview

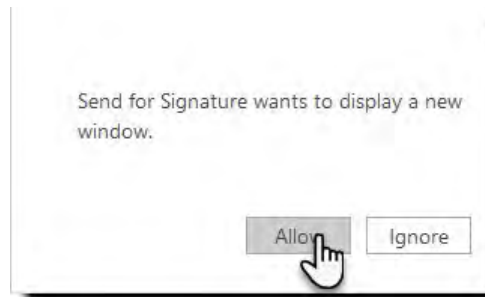
The *Adobe Sign for Outlook* add-in allows a user to configure a new agreement from within their email client by either composing a new email, starting from a blank slate, or by replying to an existing email, importing the recipient list, and automatically attaching any files from the source email.

This document is broken into three parts:

- **Installing/Enabling the add-in on your Outlook account** – The one-time process for enabling the add-in from the 365 store. All users should be able to do this without elevated system permissions.
- **Establishing the authenticated connection between Outlook and Adobe Sign** – Once the add-in is enabled, a trust relationship between Microsoft and Adobe Sign has to be created. This is done by authenticating to both environments, and only needs to be established one time.
- **Using the add-in** – This section explores the features of the add-in and how you can use it to leverage Adobe Sign directly from your email client.

365 Admins can centrally [install the add-in at the tenant level](#), and control access at the user level if desired.

Note: During authentication and use of the add-in, Outlook 365 will prompt an authorization panel when attempting to open a new window. When this happens, click **Allow**.



ON THIS PAGE

[Overview](#)[Prerequisites](#)[Enabling the add-in](#)[Establishing the authenticated relationship](#)[Using the add-in](#)[Add-in Settings](#)[Installing at the Tenant level](#)Applies to: **Sign**Last Published: **June 21, 2018**

Prerequisites

Supported products:

- Exchange Online

Clients:

- Outlook 2013 (Windows v15+)
- Outlook 2016 (Windows v16+)
- Outlook Online – Using:
 - Chrome v59+
 - Firefox v53+
 - Safari 9+
 - Edge 38+
 - IE 11+
- Outlook 2016 (Mac v15.35+)

You also need to comply with the basic [Microsoft requirements to use Office](#)

Note: This add-in is not supported in mobile browsers and mobile apps

For the add-in to properly work, cookies **must** be enabled in the browser.

Use of the Desktop application requires that cookies be enabled in Internet Explorer.

Pop-up blockers must be disabled to use the automatic reply aspect of the Fill and Sign feature.

IE/Edge browsers

For the add-in to work seamlessly in Internet Explorer and Edge browsers, you must trust the below sites in your browser security configuration:

- https://*.echocdn.com
- https://*.echosign.com
- https://*.microsoftonline.com
- https://*.office.com
- https://*.office365.com
- https://*.live.com (If using a Live account)
- https://*.sharepoint.com
- If using a third-party identity management system, that URL needs to be added as well

Mac High Sierra OS

High Sierra users may encounter an issue while trying to access the add-in from the Outlook desktop app (version 16.11 up) that throws a generic error message from Adobe Sign stating that the cookies are not enabled.

If this happens:

- Open the add-in [Settings](#), and **Sign Out**
- Re-authenticate to the service by clicking **Get Started**

If re-authenticating fails to correct the problem, contact customer support.

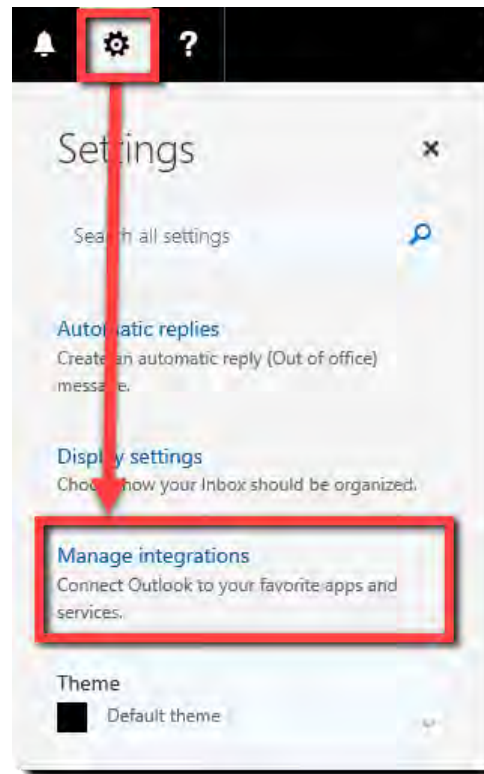
Enabling the add-in

The *Adobe Sign for Outlook* add-in can be installed in both the web based and desktop launched applications. Installing the application in one environment enables it in both

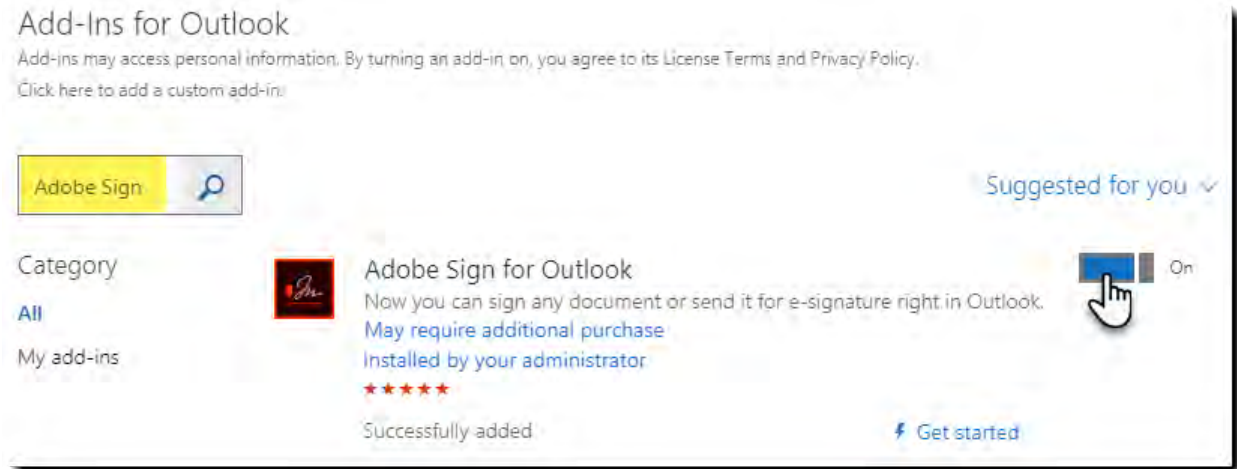
Access to the store is slightly different in each environment, and instructions are provided below for both.

Installing the add-in for OWA (the web-based client)

1. Log in to your 365 Outlook account and select the **Mail** option
2. Click the gear icon in the upper-right corner of the screen
3. Select the **Manage integrations** option to load the *Add-ins for Outlook* page



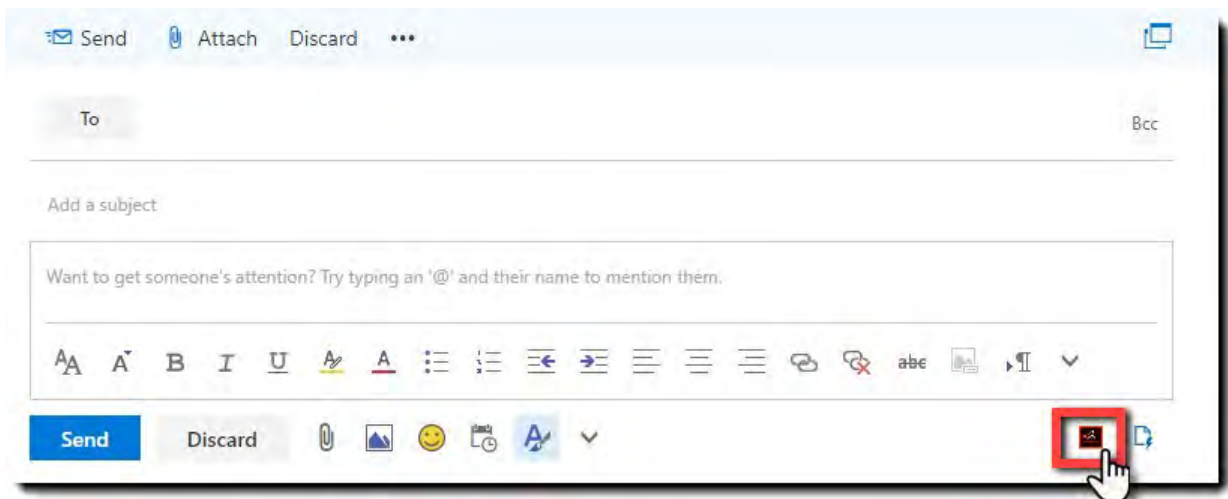
4. In the top left search box, type **Adobe Sign** and click the search icon
5. To the right of the **Adobe Sign for Outlook** option, click the **On** button enable the integration
 - Once done, you should see *Successfully added* below the integration



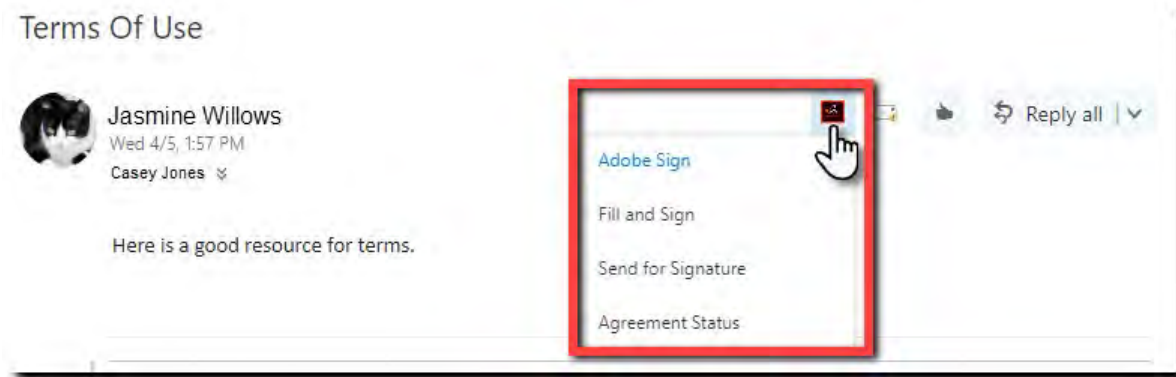
6. Close the *Add-ins* page

To access the add-in, open any email. You will find the Adobe Sign icon in one of two places:

- **New emails** – The interface to compose a new email exposes the icon in the lower-right corner of the screen
 - New emails only have the option to *Send for Signature*



- **Reply emails** – When replying to an email, the icon is found in the upper, mid-right corner of the window (depending on how many add-ins you have installed)

**Note:**

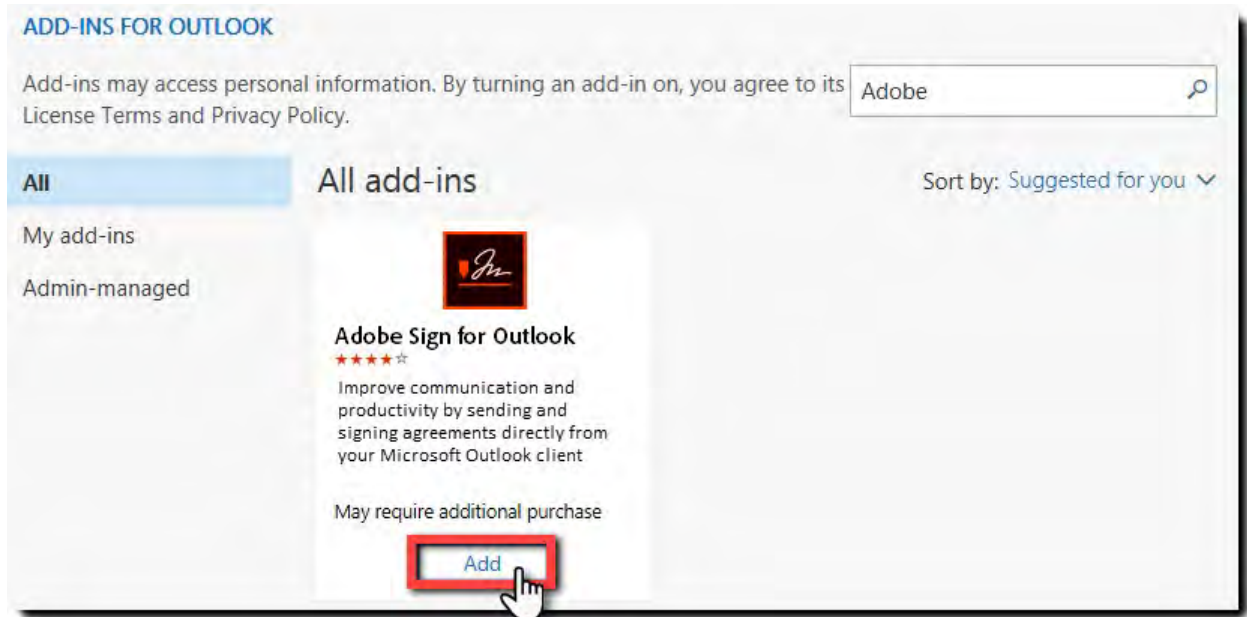
When you invoke the add-in from a Reply email, a pop-out menu will appear prompting you to select one of three functions (as described in [Using the add-in](#) section).

Installing the add-in for the desktop Outlook client

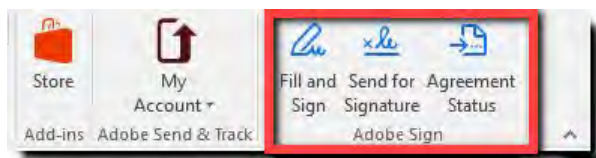
1. Open your desktop Outlook application
2. Navigate to the **Home** tab, and click the **Store** icon in the *Add-ins* section



3. In the top left search box, type **Adobe** and click the search icon
4. When you find the **Adobe Sign for Outlook** option, click the **Add** button to enable the add-in
 - Once done, you should see *Added* and a blue check indicating the add-in is available



After enabling the add-in, you will find a new *Adobe Sign* section (with three icons) in your ribbon on the *Home* tab:



Establishing the authenticated relationship

Once the add-in is enabled within the email client, you must create a relationship between your Microsoft account, and your Adobe Sign account. This ensures that you, and only you, are sending agreements through your Adobe Sign user.

The configuration process is quick, and only requires that you know how to authenticate to the two systems.

Note:

Once you have established this relationship, you do not need to authenticate again to either system. The authenticated relationship is persistent unless explicitly deleted by [signing out of the add-in](#).

To establish the trust:

1. Click the **New Email** button as if you were composing a new email

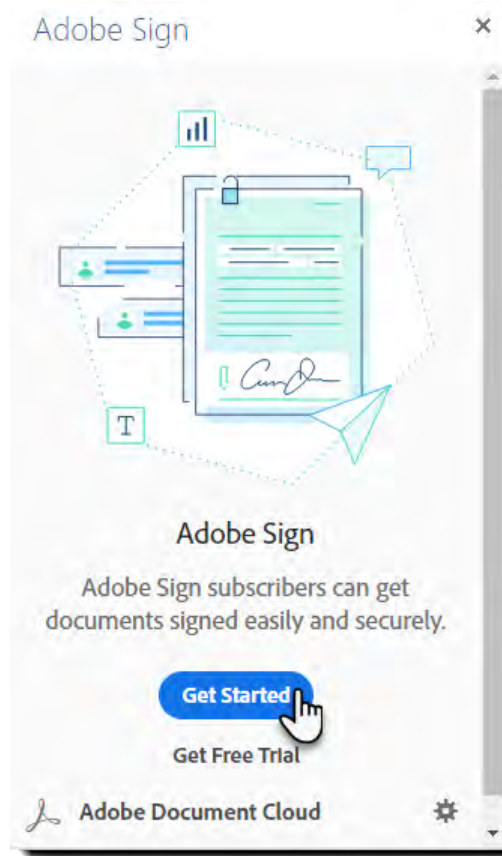
2. Find the Adobe Sign icon in the email page layout and click the **Send for Signature** option

- This opens the add-in panel on the right side of the window



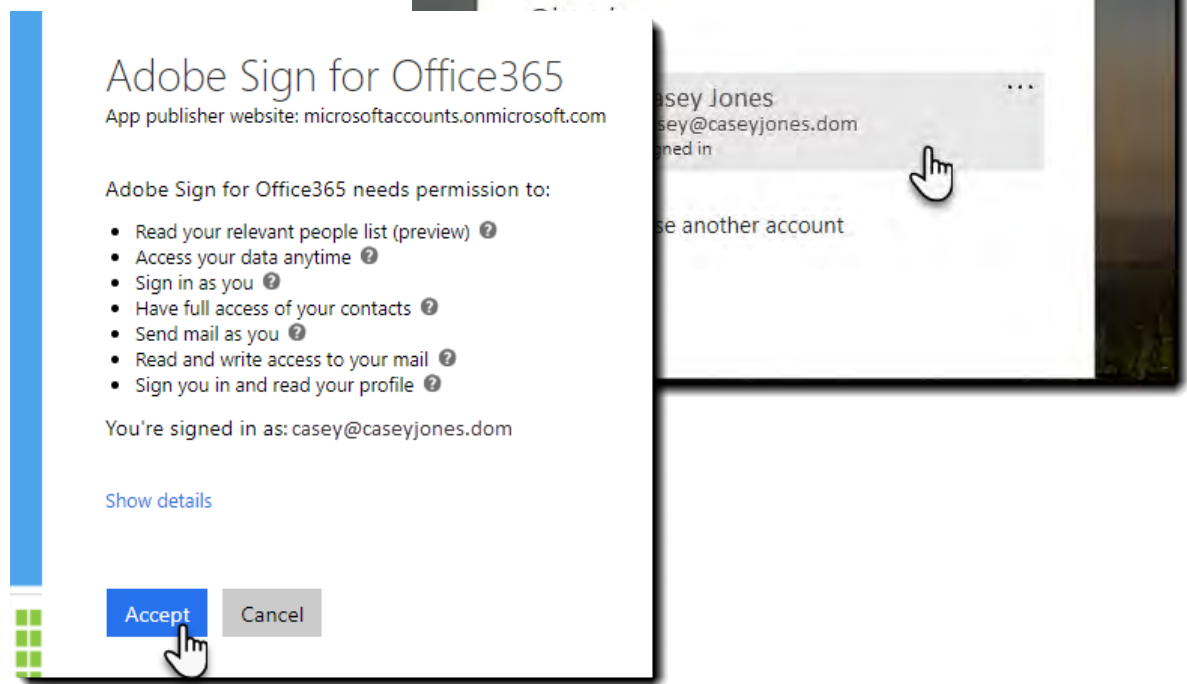
3. Click the **Get Started** button in the add-in panel

- The *Get Free Trial* link opens a new window to the [Adobe Sign 30-day free trial registration](#) page. If you don't already have an Adobe Sign account, sign up for the free trial before you continue. No billing information is collected, and there is no commitment to pay anything during or after the trial.



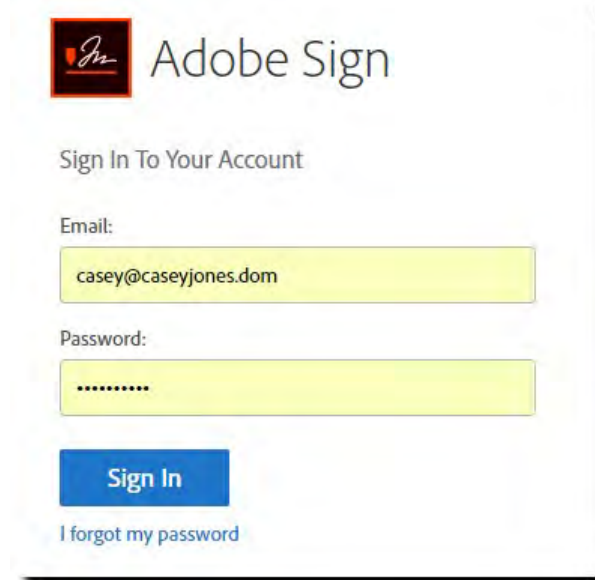
4. You may be prompted to authenticate into the 365 environment. Click the user you intend to use. (The user you are already authenticated as will be at the top of the list)

5. Office 365 then prompts you to grant access to the add-in. Click **Accept**



A new window opens to capture the authentication for Adobe Sign.

6. Authenticate using your **Adobe Sign** credentials.

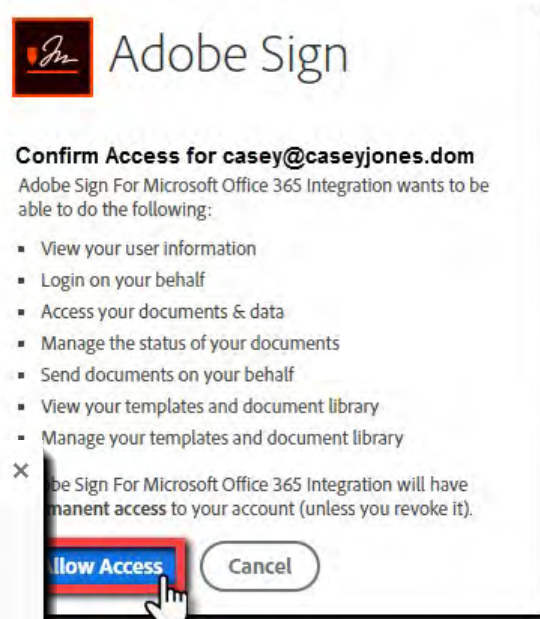
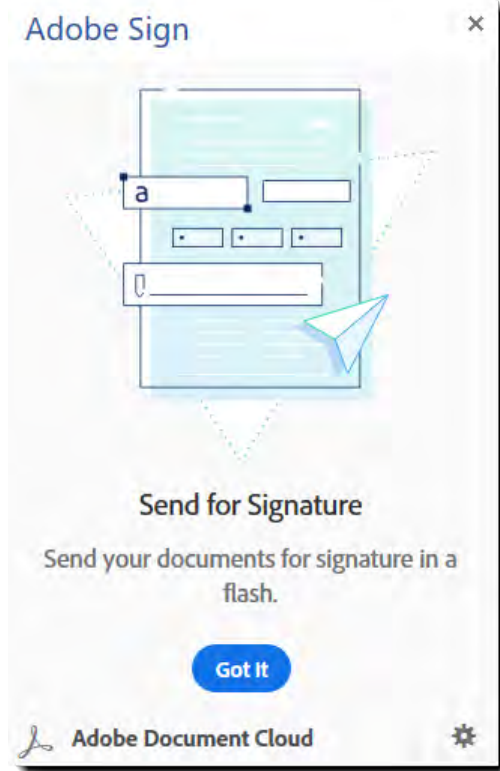


7. After authentication to Adobe Sign, you are asked to confirm the access. Click **Allow Access**

Once the Adobe Sign authentication is successful, the add-in panel on the right changes to show the add-in splash page. Click **Got It** to open the configuration panel.

The trusted relationship is in place and will remain functional until you [sign out of the add-in](#).

Disabling/uninstalling the add-in does **not** delete the trusted relationship.



Using the add-in

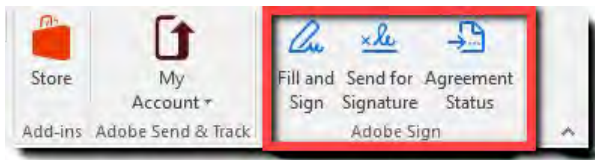
With the trust relationship to Adobe Sign established, you can start sending agreements directly from your email client.

In the context of this add-in, Outlook has two modes:

- **Compose** – Compose mode is anytime you can type/add to the email. This is generally achieved by clicking the *New* button, to start a new email, or the *Reply* button when replying to an existing email thread
 - When in compose mode, only the *Send of Signature* feature is available



- **Read** – Read mode is any time you are viewing an email, but cannot edit/author it
 - Read mode enables three features:



1. **Fill and Sign** – A feature that allows the sender (and only the sender) to add content to, sign, and optionally send a file to another party as a completed document
2. **Send for Signature** – Creates an agreement that can have one or multiple recipients other than the sender. The sender may be a recipient, just not the *only* recipient
3. **Agreement status** – This option displays a list of the last ten agreements that include the user, including *Draft*, *Out for Signature*, *Waiting for me to sign*, and *Signed*

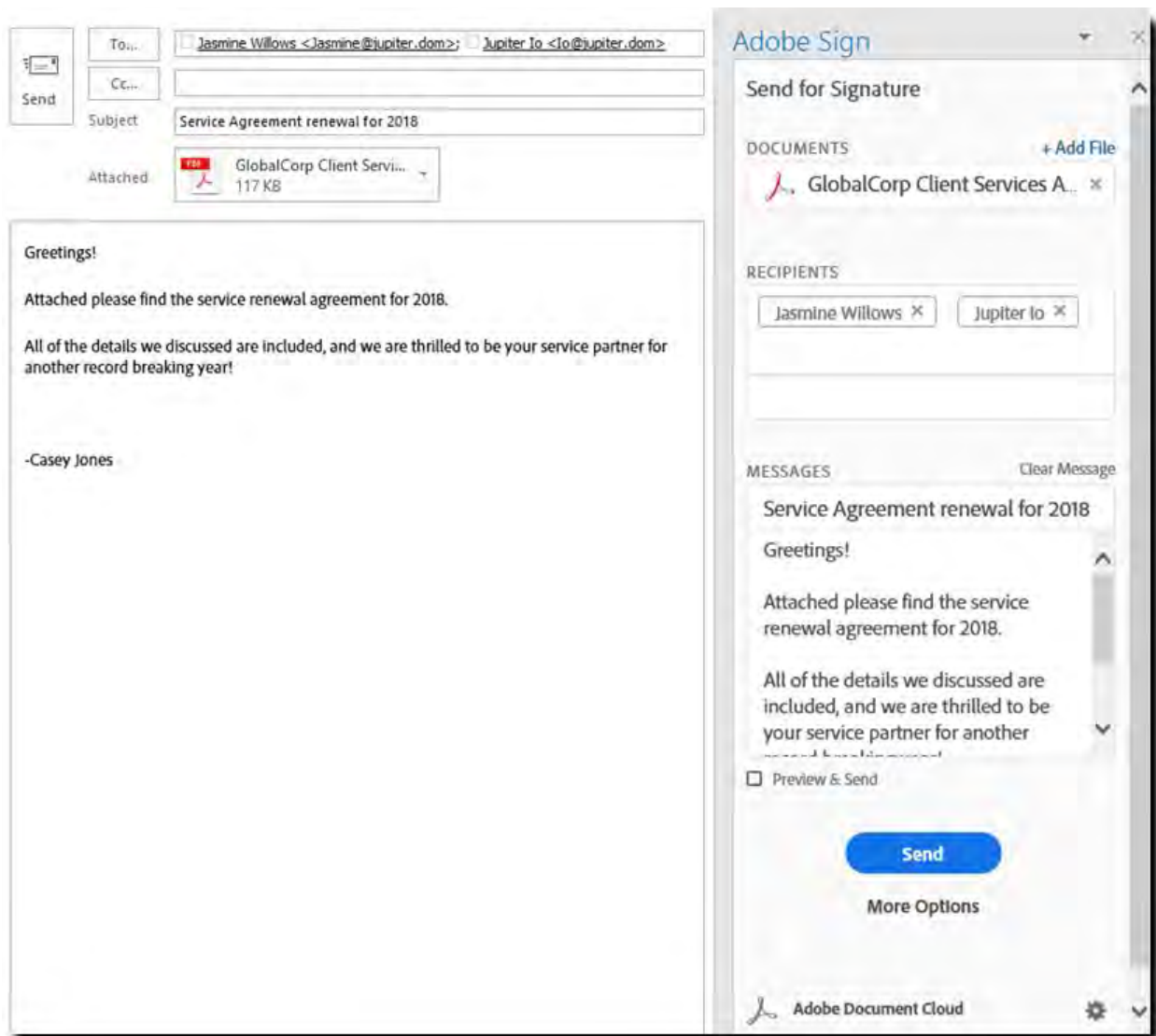
Sending from “Compose mode”

When launching the add-in from an email, the add-in seeks to include values from the email itself. Composing a new email (either from clicking the *New* or *Reply* button) allows you to configure that email as a template *before* launching the add-in, making short work of renewals, and other boilerplate transactions.

- If an attachment is included in the email, the add-in attempts to attach that same file as the agreement document
- If there are recipients listed in the TO: field (other than the sender), those emails will be imported as the recipient list, in the order they appear in the TO: field
- If there is content in the Subject line, that literal string will be used as the Agreement Name.
- If there is content in the body of the email, that content will be imported as the Agreement Message

Note:

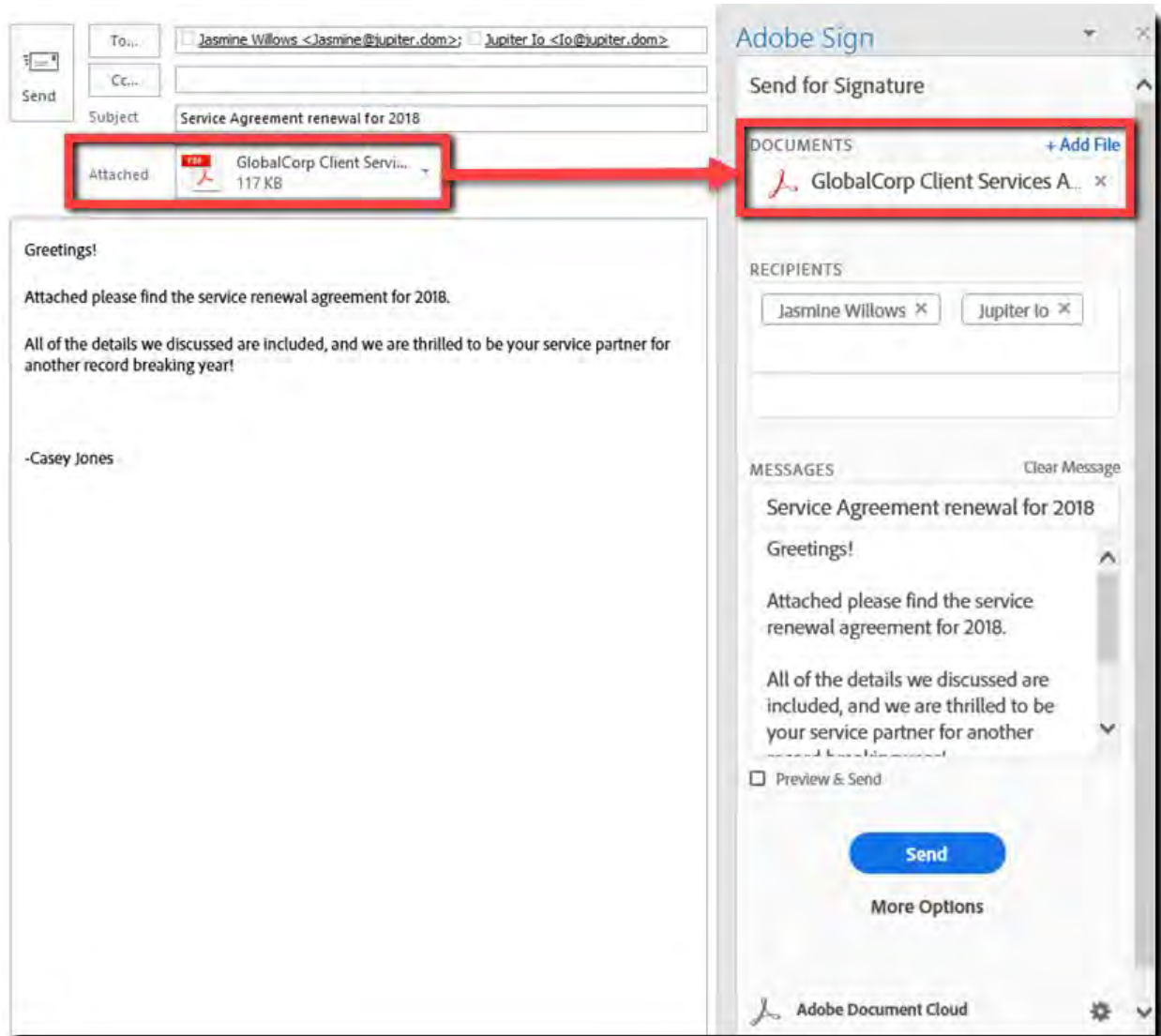
All fields can be manually added to or edited. Importing values from the email is an optional perk, not a requirement.



Documents

At the top of the add-in panel is the *Documents* section. These are the files that are attached to the agreement, and presented to the recipients for their signature.

- If you launch the add-in from an email with an attachment on it, that attachment is automatically inserted into the document list
- If you want to remove a file from the *Documents* list, click the X on the far right of the document file name



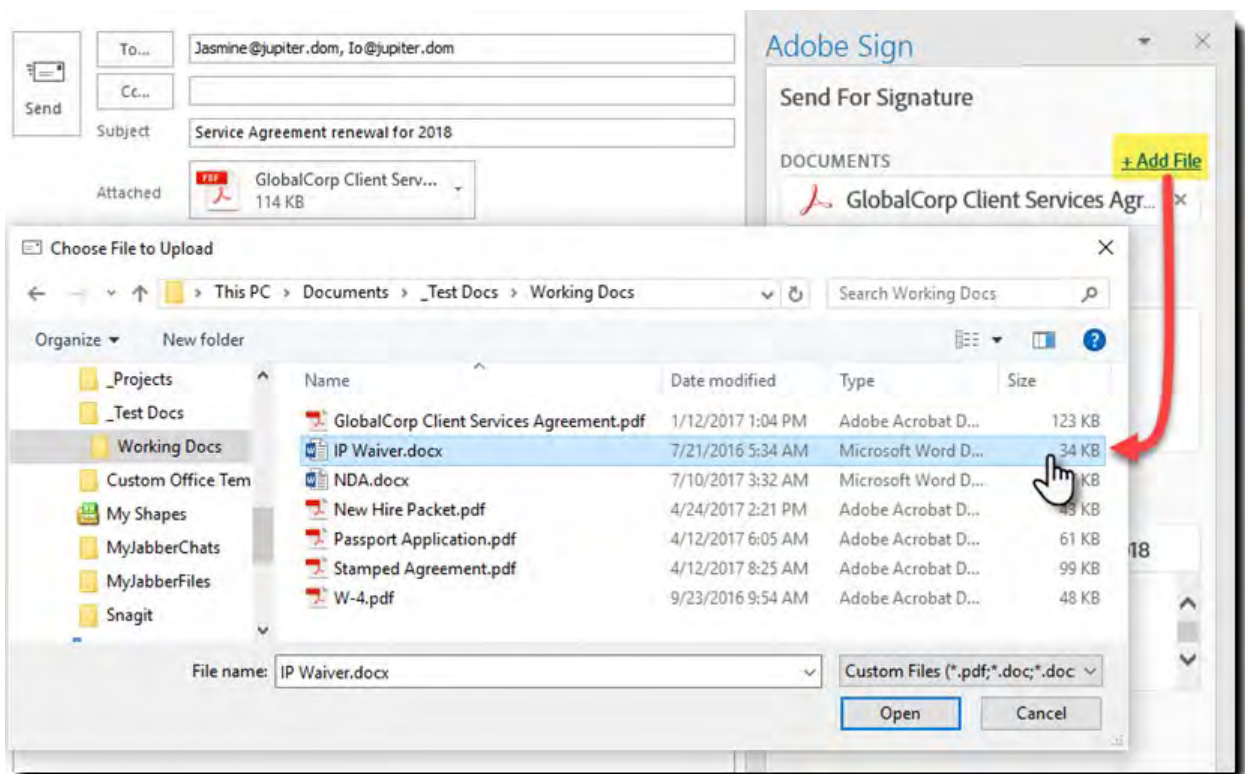
Just to the right of the *Documents* heading is the **+ Add Files** link that allows you to add files to the agreement.

- The documents are presented to the recipients in the order they are listed in the add-in panel
- If you need to add files from your Adobe Sign library, click the **More Options** link

Supported file formats:

- | | |
|----------------------------|------------|
| • Word (.doc, .docx) | • TIF/TIFF |
| • PowerPoint (.ppt, .pptx) | • JPG/JPEG |
| • Excel (.xls, .xlsx) | • BMP |
| • PDF | • GIF |
| • HTML | • PNG |

- RTF

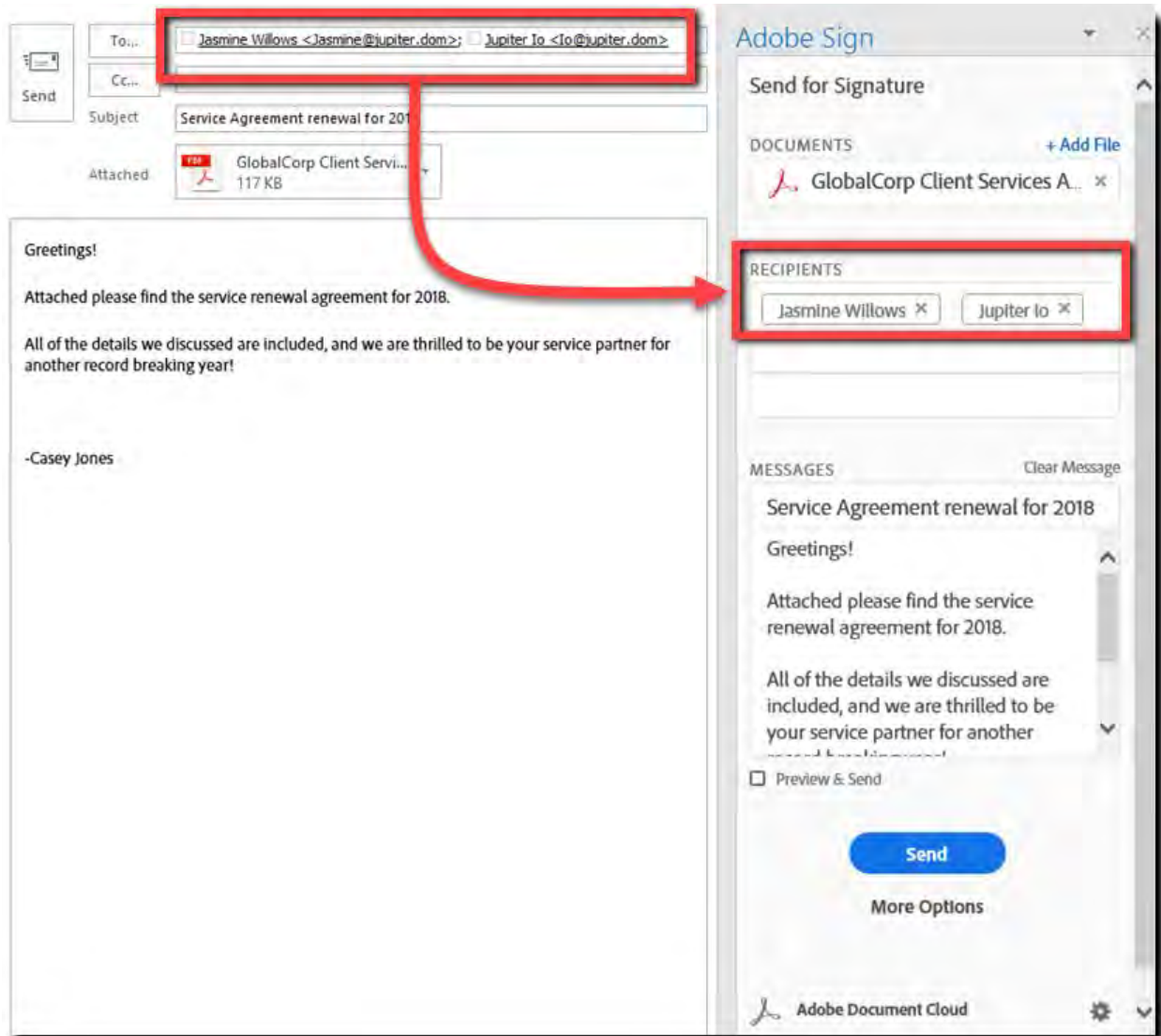


Recipients

Under the *Documents* list is the *Recipients* list.

The order that the recipients are listed in governs the order that the recipients will be asked to sign the agreement (in a sequential workflow).

- If you launch the add-in from an email that has the *TO:* field configured, the recipients are imported to the add-in panel in the order they are listed in the *TO:* field
- Recipients can be typed directly into the add-in panel
 - The panel will reference your Outlook contact list and attempt to match what you are typing to a known contact
- All recipients have the role of *Signer*
 - If you need to set different recipient roles, or send using a parallel/hybrid workflow, click the **More Options** link
- All signer verification Email.
 - If you need to use a second factor verification method, click the **More Options** link



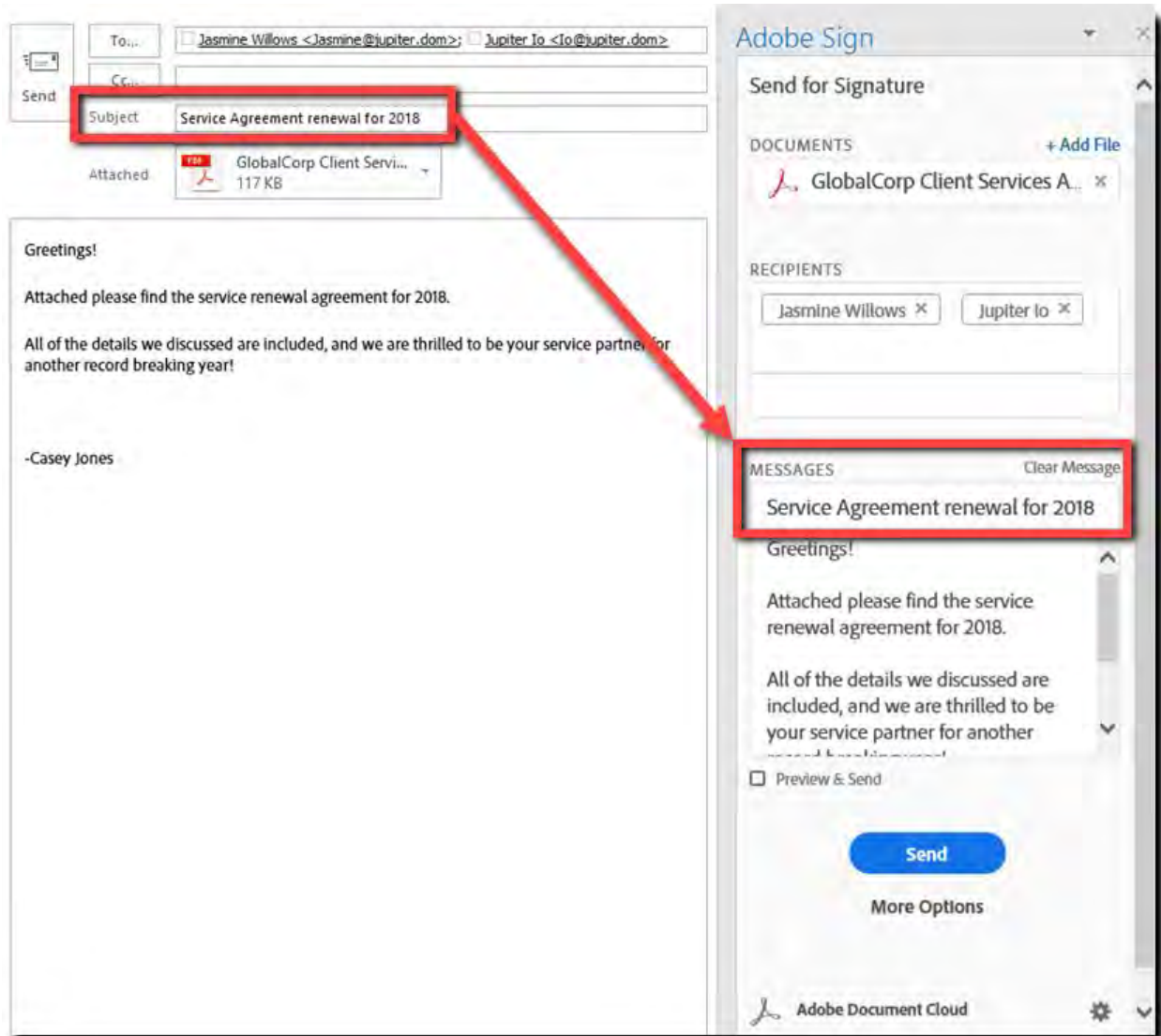
Agreement Name / Messages

The *Messages* section is under the *Recipients* list.

There are two fields in this section:

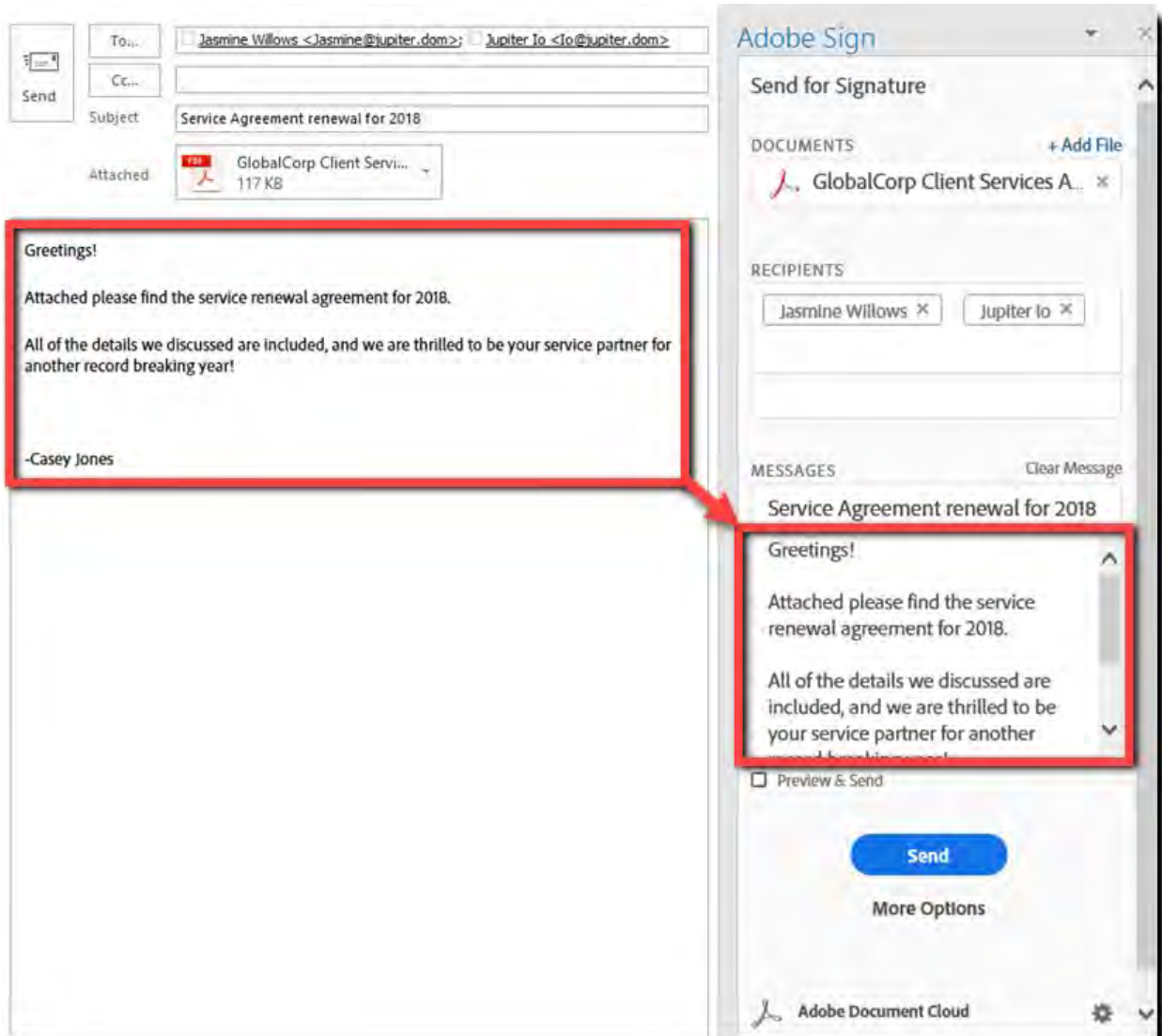
The Agreement Name is the top field.

- If you are launching the add-in panel from an existing or configured email, the *Subject* line is imported as the agreement name
- If there is no *Subject* content, the name of the first attached (*Document*) file is inserted as the agreement name
- The agreement name can be manually edited at any time



The second field is the Agreement Message that is included in the *Please Sign* email.

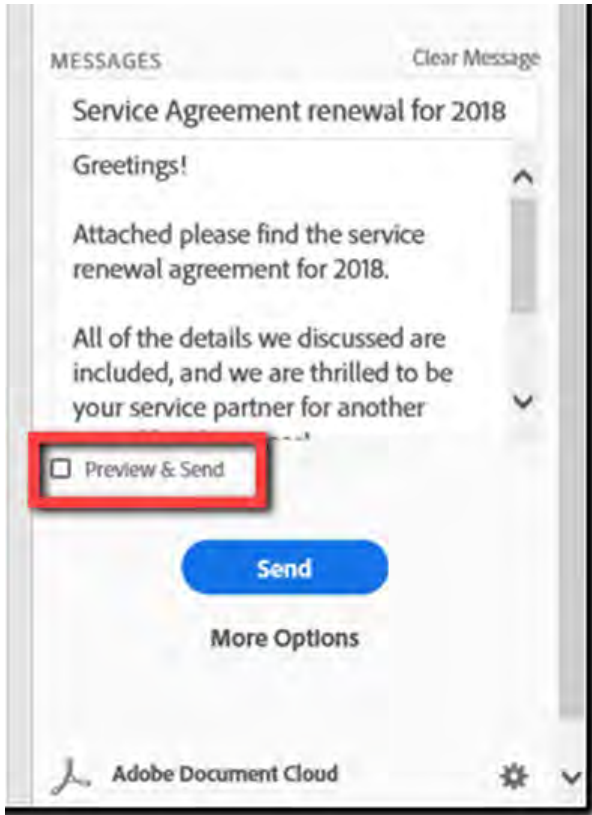
- When the agreement is launched from an existing email, the body content of the email is inserted into the message field
- If there is no content in the email body, a default message is entered: *Please review and complete this document.*
- The Message field has a 1000-character limit
- In the top right corner of the *Message* section is a **Clear Message** link that will remove all the content from the *Message* window
- If you use *Message Templates* or *Private Messages*, use the **More Options** link



Preview & Send

The *Preview & Send* checkbox invokes the Adobe Sign authoring environment once the *Next* button is clicked.

- Checking the *Preview & Send* checkbox changes the text of the *Send* button to "Continue"
- Unchecking the *Preview & Send* checkbox reverts the *Continue* button back to *Send*

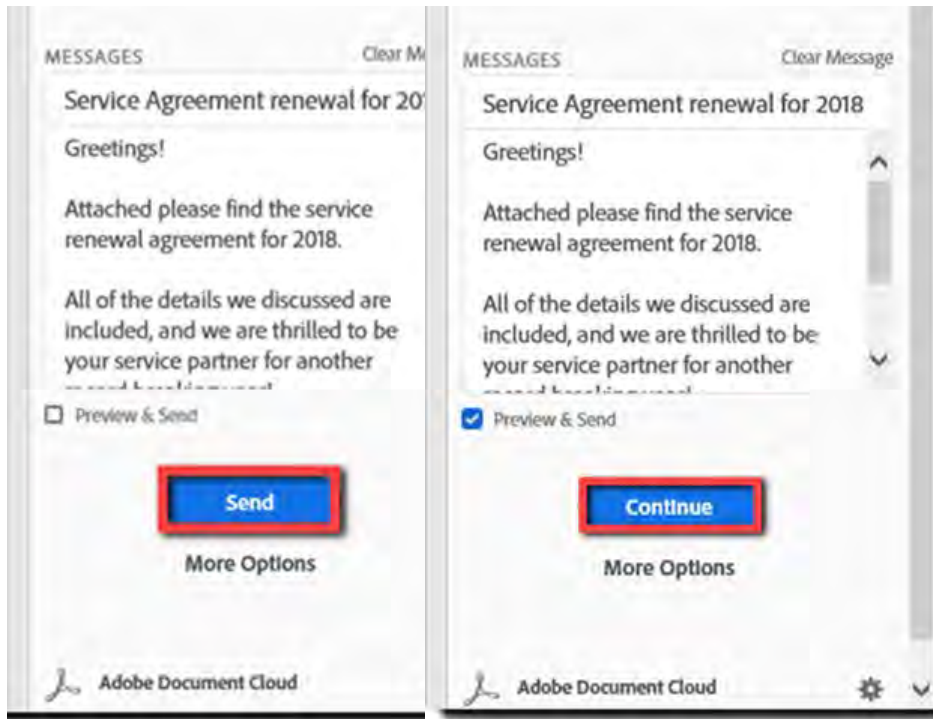


Send / Continue

This button commits the agreement to the next step, either starting the signature cycle, or opening the authoring environment, depending on how the add-in panel is configured.

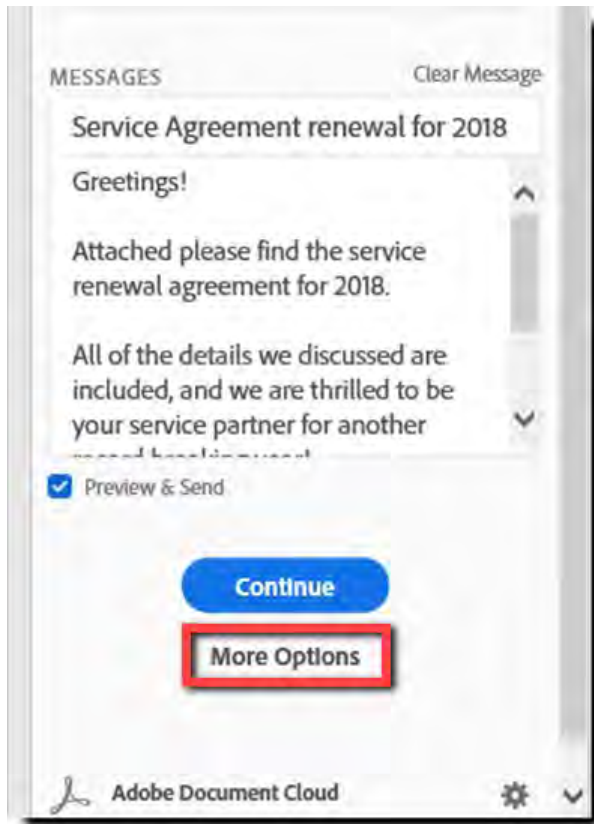
The text of the button tells you what to expect:

- **Send** – The *Send* button ends the configuration stage, and launches the agreement, notifying the first recipient.
- **Continue** – When the *Preview & Send* checkbox is checked, the button text changes to *Continue*
 - Clicking the *Continue* button opens the Adobe Sign authoring environment where you can review the document order, and place form/signature fields as needed
 - After reviewing the document and/or placing any fields, the agreement is launched to the first recipient by clicking *Send* on the authoring page. You are **not** returned to the add-in to launch this agreement.



More Options

Adobe Sign offers a wider set of options than can reasonably be installed into an add-in. Features like recipient roles and private messages over complicate the relatively small footprint that the add-in occupies. But for many, those options are critical to the business process.










The *More Options* link, just under the *Send/Continue* button, opens a windowed instance of the Adobe Sign *Send* page, complete with all options available to your account.

All the configured elements in the add-in panel are imported to the *Send* page, in the order they exist, and they are fully editable if you need to make adjustments.

Recipients

Complete in Order ☒ Complete in Any Order ☐ [Add Me](#) [Add Recipient Group](#) [?](#)

1	 <input type="text" value="Jasmine@jupiter.dom"/>	 <input type="text" value="Email"/>	
2	 <input type="text" value="lo@jupiter.dom"/>	 <input type="text" value="Email"/>	
	 <input type="text" value="Enter recipient email"/>		

[Show CC](#)

Message


Service Agreement renewal for 2018

Greetings!

Attached please find the service renewal agreement for 2018.

All of the details we discussed are included, and we are thrilled to be your service partner for

Files [Add Files](#)

 GlobalCorp Client Services Agreement.pdf

Drag More Files Here

☒ Preview & Add Signature Fields

[Next](#)

Options [?](#)

☐ Password Protect

☐ Completion Deadline

☐ Set Reminder

Signature Type

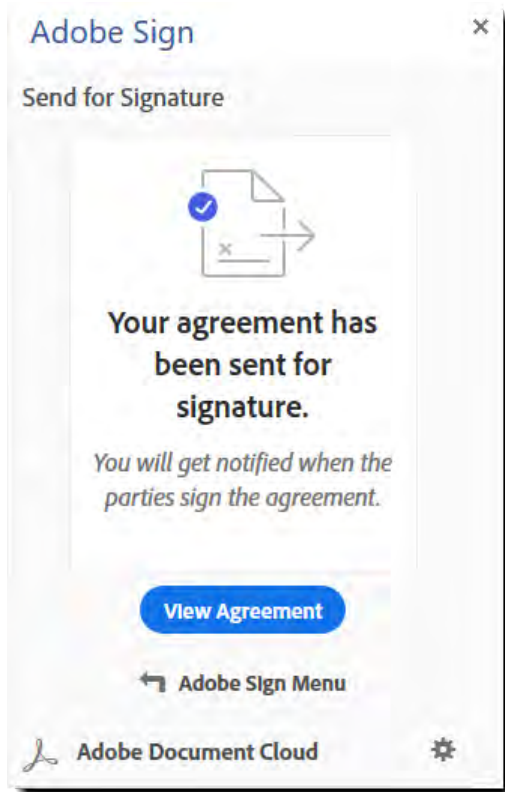
☒ Electronic ☐ Written

Recipients' Language

Once the agreement is sent, the add-in panel presents a success notification.

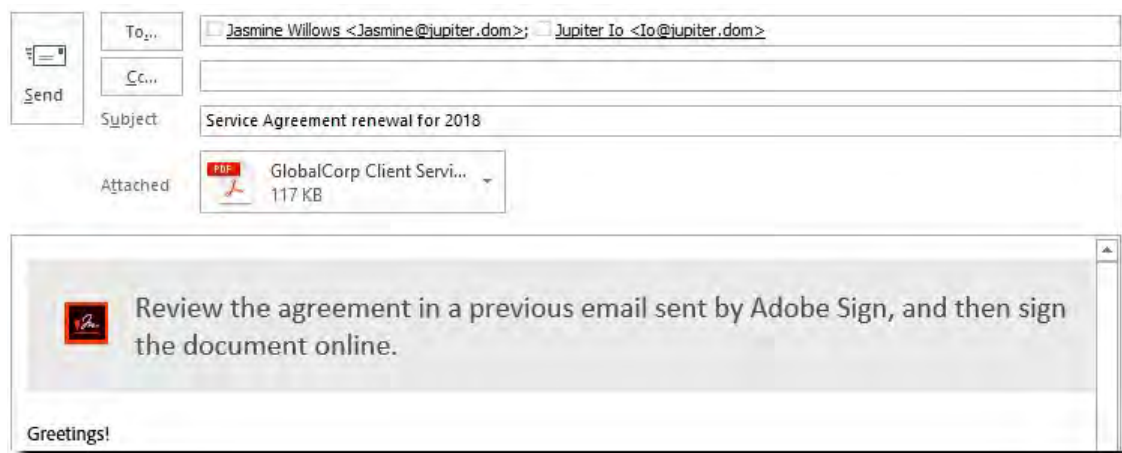
Two options are available in the post-send panel:

- **View Agreement** – Opens a windowed view of the agreement that was just sent
- **Adobe Sign Menu** – This option changes the panel to show the add-in feature options
 - Send for Signature



Additionally, a banner is added to the email body, indicating that the agreement is available to sign in a separate email.

This is provided in the event that the sender wants to send a follow-up email to the one auto-generated by the Adobe Sign system.



Sending from “Read mode”

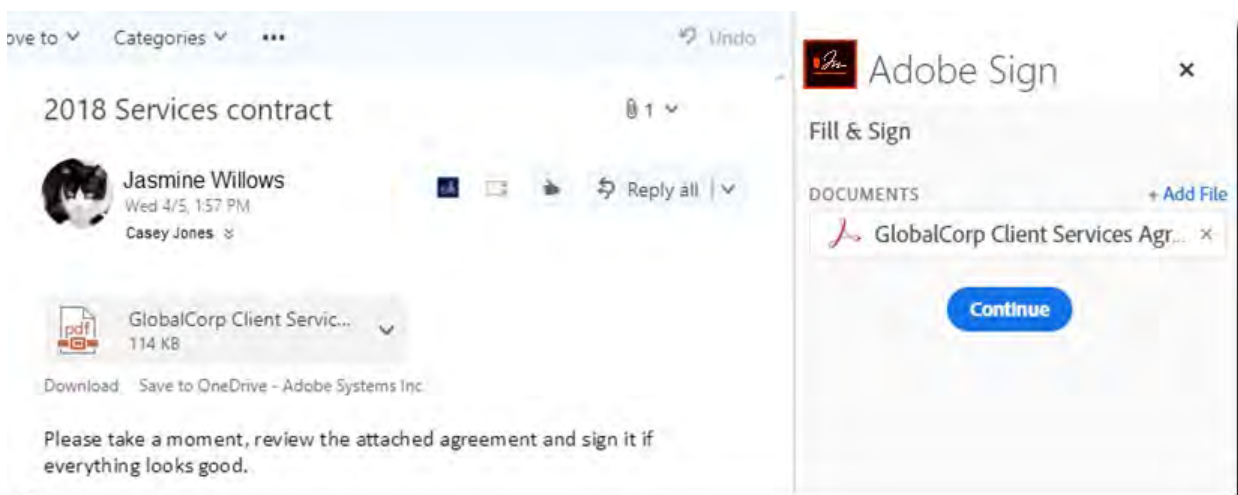
When reading an existing email thread, you have three feature options:

- **Fill and Sign** – Used when you, and only you, need to fill in a document and apply a signature. No other signers are involved. If you get a request to “Fill this out, sign it and send it back to me”, this is the option you are looking for.
- **Send for Signature** – The standard sending process for an agreement where the sender is not the sole signer
- **Agreement Status** – Shows the status of the last ten agreements involving the user

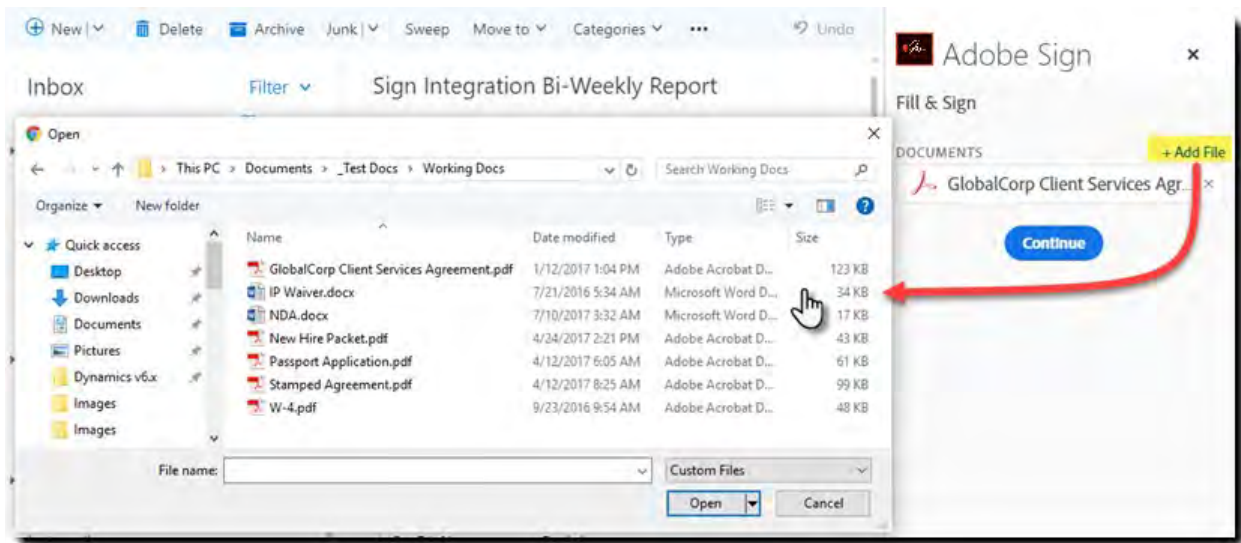


Fill and Sign

When the *Fill and Sign* option is selected, the attachment on the email (if any) is automatically attached to the agreement definition being built in the add-in panel on the right side of the window.



Just to the right of the Document heading is the **+ Add Files** link that allows you to add more files to the agreement. Adding agreements works just like the web application. The documents are presented to the signer in the order they are listed in the add-in panel



Once all the files are attached, click the **Continue** button to launch the *Fill and Sign* window

Client Information			
Company Name			
Address		Contact	
Phone		Email	
Fax		Website	
Order Number			

The *Fill and Sign* window allows you to:

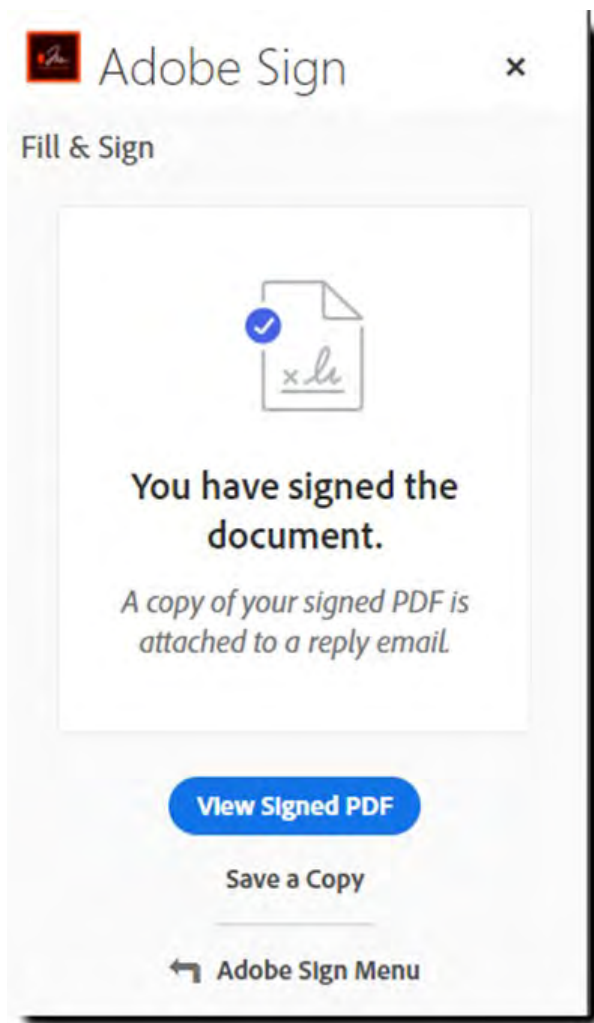
1. Type in text by clicking anywhere on the form and typing

2. Place checks or solid dots (for check boxes)
3. Apply your signature
4. Apply your initials

For more information on the Fill and Sign properties, [check out this guide](#).

When the document is completed, click the **Done** button in the upper-right corner.

The document will process for a moment, and then open a *Reply* email with the signed copy of the document already attached.



The add-in panel will show a success message that you have signed the document, and present you with three options:

- **View Signed PDF** – Opens a view of the signed PDF
- **Save a Copy** – Downloads a copy of the signed PDF to your local system
- **Adobe Sign Menu** – This option changes the panel to show the add-in feature options

- Fill and Sign
- Send for Signature
- Agreement Status

Send for Signature

1. When starting an agreement from an email with an attachment, notice that at top of the panel is the list of *Document* files currently "attached".

By default, any file that is attached to the email when the *Send for Signature* icon is clicked, is automatically attached.

- Deleting that default file is perfectly fine.
- Adding additional files is also permitted via the **Add Files** link

2. Just below the *Documents* section, the *Recipients* are listed. Recipients are **not** imported from the email in *Read* mode.

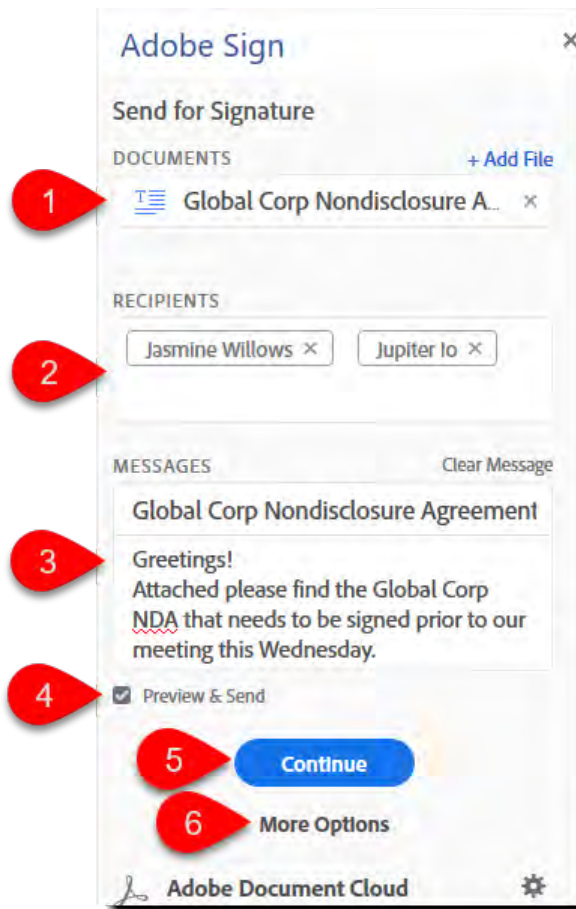
Click into the white field under the *Recipients* heading, and start typing either a name or email address. The add-in shows contacts from your 365 account that match the string you have typed in, helping to find the right recipient.

The order that the recipients are entered dictate the signature order of the agreement (in a sequential signing process).

Note: If you are accustomed to setting recipient roles, be aware that all recipients are considered **Signers** when configured in the add-in. If other roles are required, click the **More Options** link under the *Send / Continue* button.

3. Under the *Recipients* list is the *Message* section, consisting of two fields.

The top field is the *Name* of the agreement. By default, this field adopts the name value of the first file attached to the agreement. It can be manually changed to any value desired.



The second field is the *Message* text. A default value is entered and can be edited freely.

4. Just under the *Message* field is the optional *Preview & Send checkbox*. Checking this box opens a windowed version of the authoring page, exposing all the standard fields and tools for creating forms.






The authoring page does not open until the *Continue* button is clicked.

5. The *Send / Continue* button sends the agreement as currently configured. If the *Preview & Send* check box is checked, the authoring page opens, allowing fields to be placed on the document. Once all fields are placed, click the **Send** button at the bottom-right of the authoring page.

6. Under the *Send / Continue* button is the *More Options* link. Clicking this link opens a windowed version of the *Send* page in the web application, exposing all the standard options that you would see in the application. Any configuration done in the add-in panel populates to the *Send* window, and is fully editable.

Recipients

Complete in Order ☒ Complete in Any Order ☐ [Add Me](#) [Add Recipient Group](#) [?](#)

1	 <input type="text" value="Jasmine@jupiter.dom"/>	 <input type="text" value="Email"/>	<input type="button" value="X"/>
2	 <input type="text" value="lo@jupiter.dom"/>	 <input type="text" value="Email"/>	<input type="button" value="X"/>
	 <input type="text" value="Enter recipient email"/>		

[Show CC](#)

Message


Service Agreement renewal for 2018

Greetings!

Attached please find the service renewal agreement for 2018.

All of the details we discussed are included, and we are thrilled to be your service partner for

Files [Add Files](#)

 GlobalCorp Client Services Agreement.pdf

Drag More Files Here

☒ Preview & Add Signature Fields

[Next](#)

Options [?](#)

☐ Password Protect

☐ Completion Deadline

☐ Set Reminder

Signature Type

☒ Electronic ☐ Written

Recipients' Language

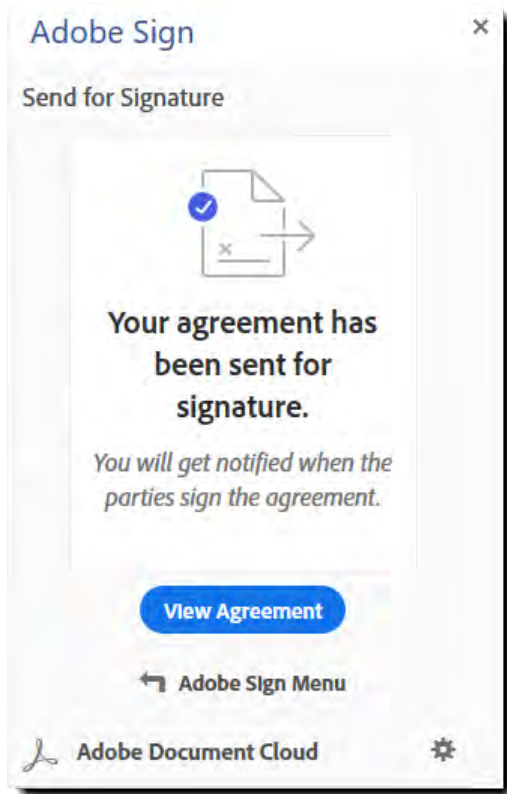
All fields and options are available just as like the *Send* page in the web application, and any changes to the recipient or file list are included in the agreement.

Scroll to the bottom of the window and click **Next** to enter authoring, or uncheck the *Preview & Add Signature Fields* box and click **Send**

Once the agreement is sent, the add-in panel presents a success notification.

Two options are available in the post-send panel:

- **View Agreement** – Opens a windowed view of the agreement that was just sent
- **Adobe Sign Menu** – This option changes the panel to show the add-in feature options
 - Fill and Sign
 - Send for Signature
 - Agreement Status



Agreement Status

The *Agreement Status* option displays the last ten agreements (based on *last update* date) that are still open and waiting for some action. This includes drafts that are waiting for authoring, agreements waiting for your signature, and agreements waiting for some other recipient.

Each listed agreement can be expanded to expose the most recent event posted for that agreement, indicating where in the signature process the agreement is.

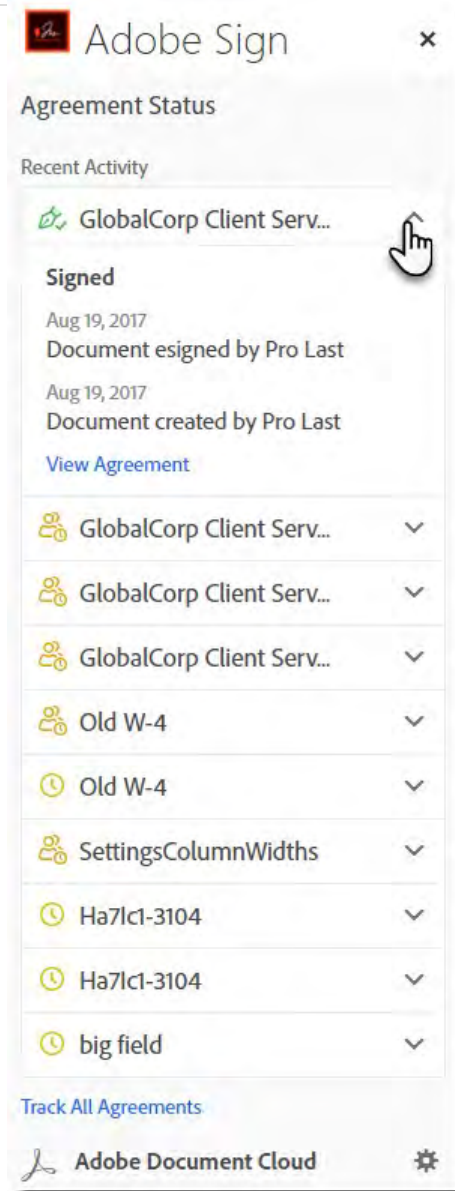
- The three most recent events logged against the agreement are listed (Created, Viewed, Signed, etc.), with the most recent on top
- Clicking the **View Agreement** link within the agreement information opens a new window showing the document in its current state
- Documents waiting for your signature display a **Sign Agreement** link that opens a new

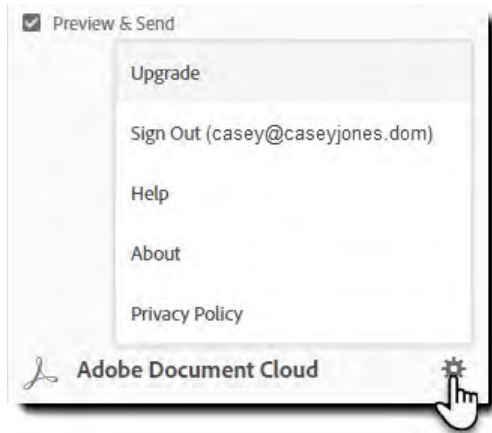
window containing the document
ready to sign

At the bottom of the events list is a **Track All Agreements** link that opens a windowed instance of the *Manage* page from the application. From the *Manage* page, the whole history of the account is available.

Add-in Settings

At the very bottom of the add-in panel, to the right of Adobe Document Cloud, is a gear icon that opens the add-in settings:





Upgrade - Trial accounts only

This link opens a new window to the Adobe Sign Upgrade process where you can purchase access to Adobe Sign on a monthly subscription.

Sign Out – Breaking the authenticated relationship

The relationship between your Outlook and Adobe Sign user accounts is “remembered” by the add-in, and this is why you don’t have to authenticate every time you use the add-in.

However, it’s not uncommon for some users to send agreements from multiple Adobe Sign accounts. This necessitates, that the user use the **Sign out** function to break the existing trusted relationship, and then establish a new relationship using the new Adobe Sign user account.

To break the relationship, click the gear icon at the bottom-right of the add-in panel. A pop-up menu appears and the Sign Out option is at the top of that menu.

Help

A link to this guide and any additional built content regarding the add-in

About

This will prompt a small pop-up that gives information regarding the add-in you are using.

Privacy Policy

This is a link to the [Adobe privacy policy](#)

Installing at the Tenant level

Installing at the tenant level allows the admin to expose the add-in by default, saving the users the installation steps, and ensuring that all users have access without issue.

Note:

The below process enables the add-in at the tenant level for the whole user base. [Check here if you would like more granular control over the deployment.](#)

The enablement is quick and easy, taking only about 5 minutes:

1. Log in as the Tenant admin, and navigate to the **Admin** panel
2. Go to the **Exchange** admin center
3. Click the **add-ins** link
4. Click the plus (+) to add a new add-in, and select **Add from the Office Store** option in the menu
 - The add-in installs as Disabled by default
5. Manually enable the add-in
 - **Make this add-in available to users in your organization**
 - When checked, the add-in is available for your users
 - If unchecked, no user in your organization will be allowed to access the add-in
 - Specify user defaults:
 - **Optional, enable by default** - The add-in is available and enabled. The user can disable the add-in if desired
 - **Optional, disabled by default** - The add-in is available, but disabled. The user can elect to enable it if they desire
 - **Mandatory, always enabled** - The add-in is available and enabled. The users have no option to disable it

Adobe Sign

☒ Make this add-in available to users in your organization

Specify user defaults:


☐ Optional, enabled by default

☒ Optional, disabled by default

☐ Mandatory, always enabled. Users can't disable this add-in.

[Save](#) [Cancel](#)

6. Click **Save** after selecting your enablement options

 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [AdChoices](#)

Adobe Document Cloud for Microsoft Office 365 and SharePoint

Deliver stand-out digital document experiences by converting manual, paper-based processes to 100% digital workflows.

Digital transformation isn't just about speeding up manual processes. It's about improving customer and employee experiences. [Adobe Document Cloud for Office 365](#), which includes [Adobe Acrobat DC](#), [Adobe Sign](#), and PDF services, integrates seamlessly with your existing business applications such as Microsoft Office and SharePoint. With this integration, you can convert paper-based processes to compelling digital experiences that impress customers and help employees work and collaborate faster.

Accomplish more in less time.

Adobe Document Cloud adds powerful PDF and e-signature tools to Office applications, so everyone in your organization can quickly collaborate on PDF documents and accelerate approval workflows.

- Access Adobe Sign and Adobe PDF tools right from the Office 365 navigation window in Outlook, Word, PowerPoint, Excel, SharePoint, and OneDrive.
- Convert Word, Excel, and PowerPoint documents to high-quality Adobe PDF files that preserve fonts, formatting, and layouts and can be optionally password protected.
- Combine multiple Office files, images, text, and PDFs into a single PDF for archiving or distribution.
- View and edit PDFs stored in OneDrive and SharePoint directly from Acrobat DC.
- Export PDF files to Excel, Word, or PowerPoint files.
- Create electronic contracts, send them for e-signature approval, and monitor status—all within Word, PowerPoint, Outlook, and Teams.
- Enable customers and employees to fill and sign documents from anywhere, on any device.

"Because of Adobe Sign, we are now able to send HR documentation to employees before they start. That's a huge savings to the state. They are being productive for the first two hours of their first day. So there's a huge return on investment for that."

TODD NACAPUY

Chief Information Officer
State of Hawaii

Increase business agility.

Speed time to market while decreasing administrative overhead and human error by automating repeatable approval and e-signature workflows within SharePoint and Flow.

- Automatically merge customer data and documents from SharePoint into electronic contracts. Send contracts for e-signature, track their progress from within SharePoint, and automatically store signed documents and any data collected during the approval process back in SharePoint.
- Route PDF documents for approval using smart SharePoint workflows with built-in logic. For example, you can automatically route contracts for signature to different or multiple approvers based on their financial value.
- Incorporate e-signatures into your favorite applications supported by Microsoft Flow. Automatically kick off tasks after an agreement is signed, and keep tabs on its status using notification templates.

"Adobe Acrobat Pro DC enables us to digitize construction drawings quickly and cost-effectively whenever someone from any of our departments needs the documents. Since we no longer have to rely on an external service provider to do the job, costs are down by 90%."

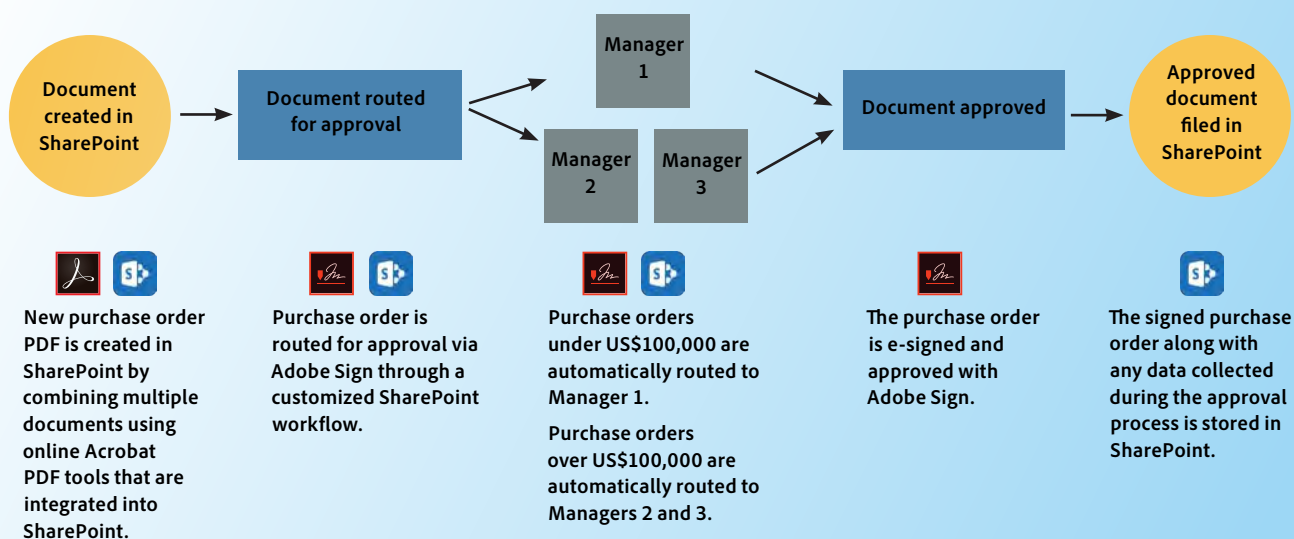
CHRISTIAN GOLTJ

Head of System Development
ASFINAG Maut Service GmbH

Deploy in no time.

Work with Office 365 admin tools to centrally deploy Document Cloud add-ins fast. For Adobe Sign and PDF services, you can use a web-based installer to configure your Office 365 accounts without installing additional software on users' desktop machines. For users who need the full desktop version of Acrobat DC, you can streamline software installation and configuration using standard tools, such as

Sample approval workflow using Microsoft SharePoint and Adobe Document Cloud



Use cases

Automate document preparation, signing, and approvals across your organization.

Sales

- Contracts and agreements
- Proposals and bids
- Application forms

Human resources

- Benefits enrollment
- New hire onboarding forms
- Policy acknowledgments

Procurement

- Vendor contracts
- RFP and bid packages
- Onboarding forms

Legal

- Nondisclosure agreements
- Business contracts
- Court e-filing and e-discovery documents

Marketing

- Communications review and approval
- Collateral publication
- Release forms

Product management

- Requirement documents
- Roadmap review and approval
- Product manuals and guides

IT operations

- Asset documentation
- Change authorization
- Policy documentation

Facilities

- Lease agreements
- Request-for-service forms
- Facilities planning

Customer service

- Service and work orders
 - Field service acknowledgments
 - Renewal agreements
-

Microsoft Windows Server Remote Desktop Services and Apple Remote Desktop. Seamless support for Single Sign-On simplifies access for authorized users. And entitlements can be centrally managed from the Adobe Admin Console, making it easy to adjust to changes in demand.

Global security, compliance, and scale.

Mitigate risk by ensuring that your documents are securely signed, managed, and stored in accordance with industry-specific compliance standards and regional regulations. Backed by hundreds of security features, processes, and controls, Adobe Document Cloud solutions are certified compliant with rigorous security standards, including SOC 2–Type 2 and ISO 27001. Documents are protected in development and in transit. And all of this runs on Adobe's scalable global cloud infrastructure.

"We use SharePoint in almost everything. So having Adobe Sign being flexible enough to be a module part of SharePoint—having that all under one roof—has made that easier for us."

MICAH HWANG

Service Delivery Specialist
State of Hawaii

The power of partnership.

Adobe and Microsoft are strategic partners. With this partnership, you can maximize your investment in Adobe and Microsoft to accelerate digital transformation across your organization, deliver exceptional customer experiences, and adapt to changing environments to meet market demand. Learn more at <https://adobe.ly/dc-msft>.



Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2018 Adobe Systems Incorporated. All rights reserved.



Adobe Sign® Voluntary Product Accessibility Template

The purpose of the Voluntary Product Accessibility Template is to assist Federal contracting officials in making preliminary assessments regarding the availability of commercial Electronic and Information Technology products and services with features that support accessibility. It is assumed that offerers will provide additional contact information to facilitate more detailed inquiries.

The first table of the Template provides a summary view of the section 508 Standards. The subsequent tables provide more detailed views of each subsection. There are three columns in each table. Column one of the Summary Table describes the subsections of subparts B and C of the Standards. The second column describes the supporting features of the product or refers you to the corresponding detailed table, "e.g., equivalent facilitation." The third column contains any additional remarks and explanations regarding the product. In the subsequent tables, the first column contains the lettered paragraphs of the subsections. The second column describes the supporting features of the product with regard to that paragraph. The third column contains any additional remarks and explanations regarding the product.

Date: 5/10/2016

Name of Product: Adobe Sign®

Contact for more Information: access@adobe.com

Guideline	Applicable	Compliance
§1194.21 – Software Applications and Operating Systems	Not Applicable	-
§1194.22 – Web-based Intranet and Internet Information and Systems	Applicable	Supports with exceptions
§1194.23 – Telecommunications Products	Not Applicable	-
§1194.24 – Video and Multimedia Products	Not Applicable	-
§1194.25 – Self-Contained, Closed Products	Not Applicable	-
§1194.26 – Desktop and Portable Computers	Not Applicable	-
§1194.31 – Functional Performance Criteria	Applicable	Supports with exceptions
§1194.41 – Information, Documentation, Support	Applicable	Supports

Section 1194.22 Web-based Internet information and applications - Detail

Criteria	Supporting Features	Remarks and explanations
(a) A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	Supports with exceptions	<p>The Adobe Sign web application provides text equivalent for some user interface components. However, a rating of Supports with Exceptions is assigned due to the following exceptions:</p> <ul style="list-style-type: none"> • The documents to be signed are rendered as images without textual equivalents. • Background images used for actionable elements such as check boxes and radio buttons do not have textual alternatives. • Multiple images and image links lack meaningful alternative text. • Simulated dialogs do not textually indicate the beginning and end of the dialog content. • Many page tab elements lack textual descriptions indicating state and role.
(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	Not Applicable	The Adobe Sign web application does not provide multimedia presentations.
(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	Supports with exceptions	The Adobe Sign web application does not always use color as the sole means to convey information. A rating of Supports with Exception is made because many page tab elements provided in the site rely on color to indicate the active state.

Criteria	Supporting Features	Remarks and explanations
(d) Documents shall be organized so they are readable without requiring an associated style sheet.	Supports with exceptions	<p>The Adobe Sign web application does not require an associated style sheet to be read. A rating of Supports with Exceptions is assigned due to the following exceptions:</p> <ul style="list-style-type: none"> • Multiple actionable elements, such as the radio buttons and checkboxes in the Send module, are provided as background images. When CSS and Background images are disabled, these controls disappear. • The site has some pages that use bold and larger fonts as implicit section headings.
(e) Redundant text links shall be provided for each active region of a server-side image map.	Not applicable	The Adobe Sign web application does not utilize server-side image maps.
(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	Not applicable	The Adobe Sign web application does not utilize client-side image maps.
(g) Row and column headers shall be identified for data tables.	Supports	The Adobe Sign web application contains modules that display information in a tabular format. The row and column headers are correctly identified.
(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	Supports	The Adobe Sign web application contains modules that display information in a tabular format. The data cells are properly associated to the data headers.

Criteria	Supporting Features	Remarks and explanations
(i) Frames shall be titled with text that facilitates frame identification and navigation	Does not support	The Adobe Sign web application has modules that contain frames. A determination of Does Not Support is made because almost all of the frames do not provide a valid title attribute.
(j) Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	Supports	The Adobe Sign web application does not display blinking or flickering page elements.
(k) A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.	Not applicable	The Adobe Sign web application does not utilize a text-only alternative page.
(l) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by Assistive Technology.	Supports with exceptions	<p>The Adobe Sign web application utilizes JavaScript to display content; although some information provided can be rendered by assistive technologies, a determination of Supports with Exceptions is made due to the following exceptions:</p> <ul style="list-style-type: none"> • Multiple simulated controls implemented with <code>div</code> tags, such as the Show Me How right menu link, and <code>anchor</code> tags without <code>href</code> attributes, such as the account holder name menu link in the top navigation bar, are not keyboard accessible. • Simulated dialogs do not textually indicate the beginning and end of the dialog content. • Many actionable elements spawn simulated dialogs without alerting users of assistive technologies of the change.

Criteria	Supporting Features	Remarks and explanations
		<ul style="list-style-type: none"> Keyboard focus does not return properly from simulated dialogs. Simulated dialogs, such as the fields' context menus when editing a document, cannot be closed from the keyboard.
(m) When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with §1194.21(a) through (l).	Supports with exceptions	The Adobe Sign web application does not require an applet or plug-in to interpret all of the pages' content. However, a rating of Supports with Exceptions is given because the application provides an actionable element to open a PDF version of documents without a link to download the reader.
(n) When electronic forms are designed to be completed on-line, the form shall allow people using Assistive Technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	Supports with exceptions	<p>Some form elements in The Adobe Sign web application are accessible to users of assistive technologies. However, a rating of Supports with Exceptions is given due to the following issues:</p> <ul style="list-style-type: none"> Multiple form field elements lack meaningful explicit labels. Many fieldset elements do not have legend elements. Some groups of form controls are missing fieldset and legend elements. Some form elements are assigned positive tabindex attribute which causes an illogical tab order on some pages.

Criteria	Supporting Features	Remarks and explanations
(o) A method shall be provided that permits users to skip repetitive navigation links.	Does not support	A determination of Does Not Support is made because The Adobe Sign web application does not provide a mechanism for skipping past repetitive navigation links.
(p) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	Supports	The Adobe Sign web application warns users before logging them off after a certain period of inactivity.

Note to 1194.22: The Board interprets paragraphs (a) through (k) of this section as consistent with the following priority 1 Checkpoints of the Web Content Accessibility Guidelines 1.0 (WCAG 1.0) (May 5 1999) published by the Web Accessibility Initiative of the World Wide Web Consortium: Paragraph (a) - 1.1, (b) - 1.4, (c) - 2.1, (d) - 6.1, (e) - 1.2, (f) - 9.1, (g) - 5.1, (h) - 5.2, (i) - 12.1, (j) - 7.1, (k) - 11.4.

Section 1194.31 Functional Performance Criteria - Detail

Criteria	Supporting Features	Remarks and explanations
(a) At least one mode of operation and information retrieval that does not require user vision shall be provided, or support for Assistive Technology used by people who are blind or visually impaired shall be provided.	Supports with exceptions	<p>The Adobe Sign web application provides accessibility information about some of its controls. It also allows keyboard access to some active elements.</p> <p>Notably, users without vision are now able to access and interact with all functionality needed to sign and submit a signed document. Because documents for signing are rendered as images, as noted in 1194.22 (a), users without vision will need to download the document to be signed in Adobe Reader to review the document and then return to the web version to complete the signing process.</p> <p>However, the rating of Supports with Exceptions is assigned due to the following issues:</p> <ul style="list-style-type: none"> As stated in §1194.22 (a), (d), (i), (n), and (l), when information about user

Criteria	Supporting Features	Remarks and explanations
		<p>interface elements is not available to assistive technologies, users of screen readers may not be able to render or interact appropriately with the controls.</p> <ul style="list-style-type: none"> • The accessibility issues listed in §1194.22 (l) affect people who are blind or visually impaired because they navigate through the application exclusively with the keyboard. • Due to the accessibility violation stated in §1194.22 (o), users of screen readers will be unable to skip past repetitive links. • As stated in §1194.22 (n), when the tab order is not logical, users of screen readers may not understand the organization or content of the page. • As stated in §1194.22 (m), users of screen readers who do not have the required version of the plug-in may have difficulty navigating to the site to download the plug-in. • Throughout the Adobe Sign web application, there are multiple same link text elements targeting different pages. • Keyboard focus that is provided to inactive elements creates confusion for users of screen reader. • Information provided in <code>title</code> attributes for simulated controls (i.e., <code>div</code>) throughout the web

Criteria	Supporting Features	Remarks and explanations
		<p>application are not rendered by screen readers. Users who are blind will not receive the information.</p> <ul style="list-style-type: none"> • In the Send module, a data table is used to lay out the page content. This is confusing to users who cannot see the visual display. • In the Send – Preview Document – Formula Dialog module, there are two sets of lists for the same list. This may cause issues for users of screen readers, who may have difficulty distinguishing between and navigating through the lists.
<p>(b) At least one mode of operation and information retrieval that does not require visual acuity greater than 20/70 shall be provided in audio and enlarged print output working together or independently, or support for Assistive Technology used by people who are visually impaired shall be provided.</p>	<p>Supports with exceptions</p>	<p>The Adobe Sign application generally provides modes of use for users with limited vision. It is assigned a rating of Supports with Exceptions because of the following exceptions:</p> <ul style="list-style-type: none"> • Some accessibility issues as listed in §1194.22 (l) affect people with low vision because they often navigate through the application exclusively from the keyboard. • In various modules within Adobe Sign, the contrast between the foreground and background colors of text is not sufficient (i.e., it is below the recommended ratio of 4.5:1). Sufficient color contrast ensures that people with low vision or color perception deficiencies and users viewing the page without color can understand page content.

Criteria	Supporting Features	Remarks and explanations
		<ul style="list-style-type: none"> As stated in §1194.22 (a) and (d), users with low vision cannot access all information when CSS and background image are disabled. As stated in §1194.22 (l), the visual keyboard focus issue affects keyboard-only users who use visual keyboard focus to determine which element has focus and what action to perform on it.
(c) At least one mode of operation and information retrieval that does not require user hearing shall be provided, or support for Assistive Technology used by people who are deaf or hard of hearing shall be provided	Supports	The Adobe Sign web application does not require user hearing for information retrieval.
(d) Where audio information is important for the use of a product, at least one mode of operation and information retrieval shall be provided in an enhanced auditory fashion, or support for assistive hearing devices shall be provided.	Supports	The Adobe Sign web application does not require user hearing for information retrieval.
(e) At least one mode of operation and information retrieval that does not require user speech shall be provided, or support for Assistive Technology used by people with disabilities shall be provided.	Supports	The Adobe Sign web application does not require user speech for information retrieval.

Criteria	Supporting Features	Remarks and explanations
<p>(f) At least one mode of operation and information retrieval that does not require fine motor control or simultaneous actions and that is operable with limited reach and strength shall be provided.</p>	<p>Supports with exceptions</p>	<p>The Adobe Sign web application provides access to multiple user interface controls to users with mobility impairment.</p> <p>Notably, users are now able to access and interact via the keyboard with all functionality needed to sign and submit a signed document.</p> <p>However, a rating of Supports with Exceptions is assigned due to the following issues:</p> <ul style="list-style-type: none"> • If form fields lack information such as labels and group labels as stated in §1194.22 (n), users of voice recognition software such as Dragon Naturally Speaking cannot access them by voicing the information about the controls. The only method to access the controls that lack accessible information is with simulated mouse actions and by navigating with the mouse grid functionality, which is tedious. • Due to the accessibility violations stated §1194.22 (o), (l), and (d), keyboard-only users are unable to access some parts of the application and cannot interact with the interface elements. • As stated in §1194.22 (l), the visual keyboard focus issue affects users with mobility impairments who use visual keyboard focus to determine which element has focus and what action to perform on it.

Section 1194.41 Information, Documentation, and Support - Detail

Criteria	Supporting Features	Remarks and explanations
(a) Product support documentation provided to end-users shall be made available in alternate formats upon request, at no additional charge.	Supports	Adobe provides electronic versions of all product support documentation.
(b) End-users shall have access to a description of the accessibility and compatibility features of products in alternate formats or alternate methods upon request, at no additional charge.	Supports	Adobe provides information on accessibility features in the documentation. Electronic versions of all product support documentation are provided.
(c) Support services for products shall accommodate the communication needs of end-users with disabilities.	Supports	Product support for Adobe products is available in a variety of formats and from a number of online sources available from Adobe Systems.

Form field validations

[Sign In](#)**SIGN** ▾

Field validations

You can set up Agreement form fields to allow that only a specific format of data can be entered.

By default, a form field allows any combination of letters, numbers, or special characters: `~!@#\$%^&*()_+--[\\{}|;':",./<>?£

Use validation if you want to only allow the entry of a specific format of data in the field. If the validation is not passed, the form will display a red warning balloon and also the form cannot be e-signed until the field is validated.

In the drag-and-drop authoring environment, you set the validation for a field by double-clicking the field and choosing an option from the **Validation** list.

Available validations are:

- String
- Number
- Date
- Time
- Zip code/postal code
- Phone
- Social Security Number

➤ E-mail address

➤ Currency

➤ Percent

▼ Custom - Regular Expression

Custom - Regular Expression - Allows for a custom validation check and error message.

Regular Expression - Used to define the check that either allows or disallows the information entered by the signer.

Error Message - The custom error message which is displayed in the red balloon warning, when validation is not met.

Note:

This concept is advanced and has many different uses depending on the situation. For a definition, visit [this page](#).

For example:

Validation	Custom - Regular Expression ▼
Regular Expression	^(?:4[0-9]{12})(?:[0-9]{3})?5[1-5][0-9]{14} 6
Error Message	Not a valid credit card number

Only valid major credit card numbers are allowed, so 1234-1234-1234-1234 fails the validation.



✓ Custom - Formula

Custom - Formula - Used to create a calculation and check against the expected entry or solution to the calculation.

Formula - Either a custom formula can be entered here, or you can use the calculation builder.

Error Message - The custom error message which is displayed in the red balloon warning, when the validation is not met.

For example:

A screenshot of the "Custom - Formula" validation configuration panel. It has three sections: "Validation" with a dropdown menu set to "Custom - Formula", "Formula" with a text box containing "fieldValue != 0" and a function button "f(x)", and "Error Message" with a text box containing "Field should not be zero".

The formula results in a validation which does not allow '0' as a value in this field.





Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region 

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [AdChoices](#)

[Sign In](#)

SIGN ▾

Adobe Sign Workflow Designer

Search Adobe Support



Search

Overview

The Workflow Designer is used to create workflows that tailor the signing processes to fit your specific business requirements. With this new tool, administrators can design and manage workflow templates easily with an intuitive drag-and-drop editor. It's easy to specify the documents to be included in an agreement; the characteristics of the participants—including predefined names, roles, and routings; form fields to be pre-filled by the sender; emails to be sent to the participants; agreement expiration or password options; and more.

Workflows also create an easy-to-follow send experiences for your users so process steps can be followed consistently every time. Senders using a workflow template are guided through the send process with custom instructions and fields, making the send process easier to use and less prone to errors.

ON THIS PAGE

[Overview](#)[What's New...](#)[Creating a custom workflow](#)[Sending using a custom workflow](#)[Signing and approving a workflow agreement](#)[Editing a custom workflow](#)Applies to: **Sign**Last Published: **June 8, 2018**

What's New...

With the June 2018 release, several changes have been applied to the Workflow Designer, bringing it closer to the functionality of the manual Send process.

The new features include the ability to:

- Use Digital signatures for one or more of your recipients
- Configure recipients to use phone-based (SMS) recipient authentication
- Configure recipient groups during the send process
- Attach documents from all enabled sources during the send process

All of the above features are enabled when you opt-in to the new *Custom Workflow Send* process.

This new send process displays in a new reflowable page, much like the Send page, and can be enabled by navigating to: **Account > Account Settings > Send Settings > Custom Workflow Send**

Note:

Please be aware that two known defects have been discovered just prior to the June release. Both are expected to be corrected with a patch in August.

1. The HTML that allowed for lists and some text formatting in the instructions is not rendering properly and displays as raw HTML on the page.

If you are not using HTML in your instructions, then this won't be evident

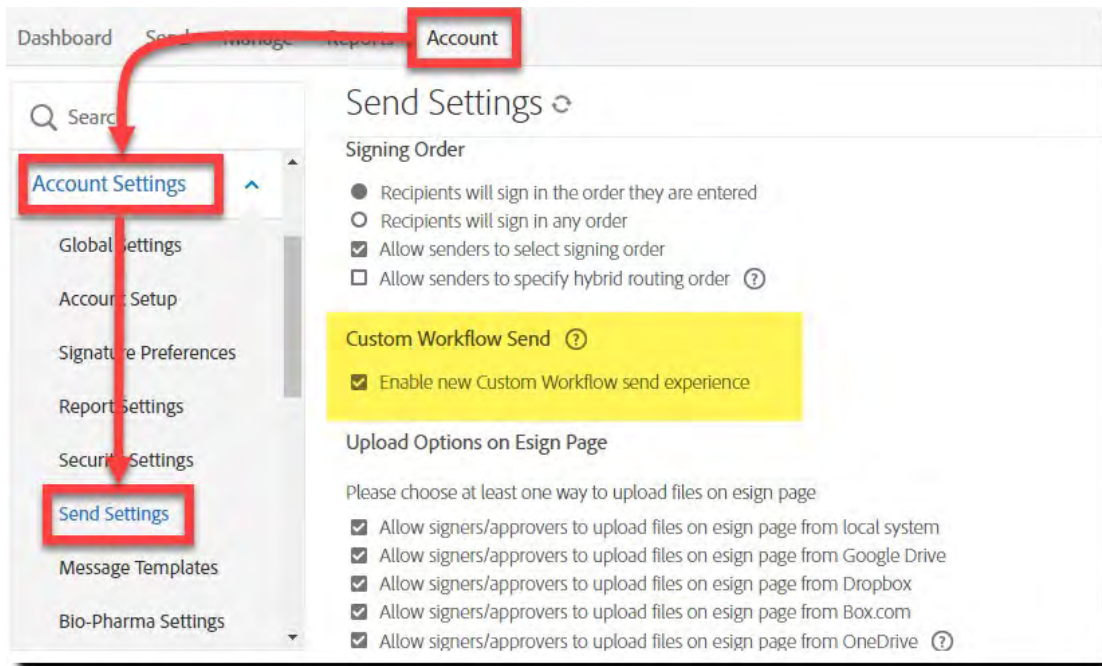
Suggested solutions:

- Remove the HTML from the instructions and update the workflow
- If the raw HTML isn't impactful, ignore it until the fix is applied in August
- Delay enabling the new workflow experience until August

2. Files that are attached in the Workflow Designer are not being automatically attached during the send process. The file must be attached manually.

The **Add File** link for the file attachment displays the file in the library (and only that file).

If having the file attached automatically is critical, do not enable the new send experience until after the August patch.



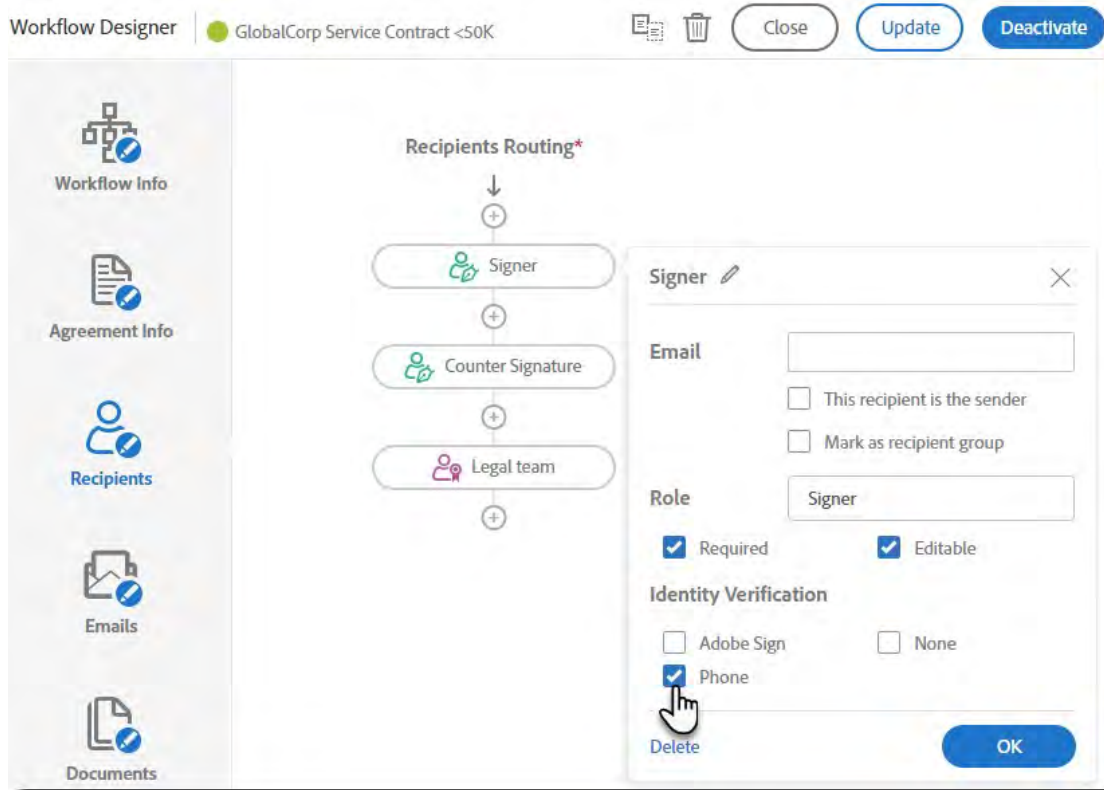
Recipient authentication

In the Workflow Designer, all the enabled authentication methods are displayed in the recipient object.

The authentication methods have been updated to display as checkboxes, allowing the workflow design to permit options for the sender.

If multiple options are checked in the designer, these same options will be available to the sender during the send process.

This release also adds phone (SMS) as an option in the designer.



Recipient groups

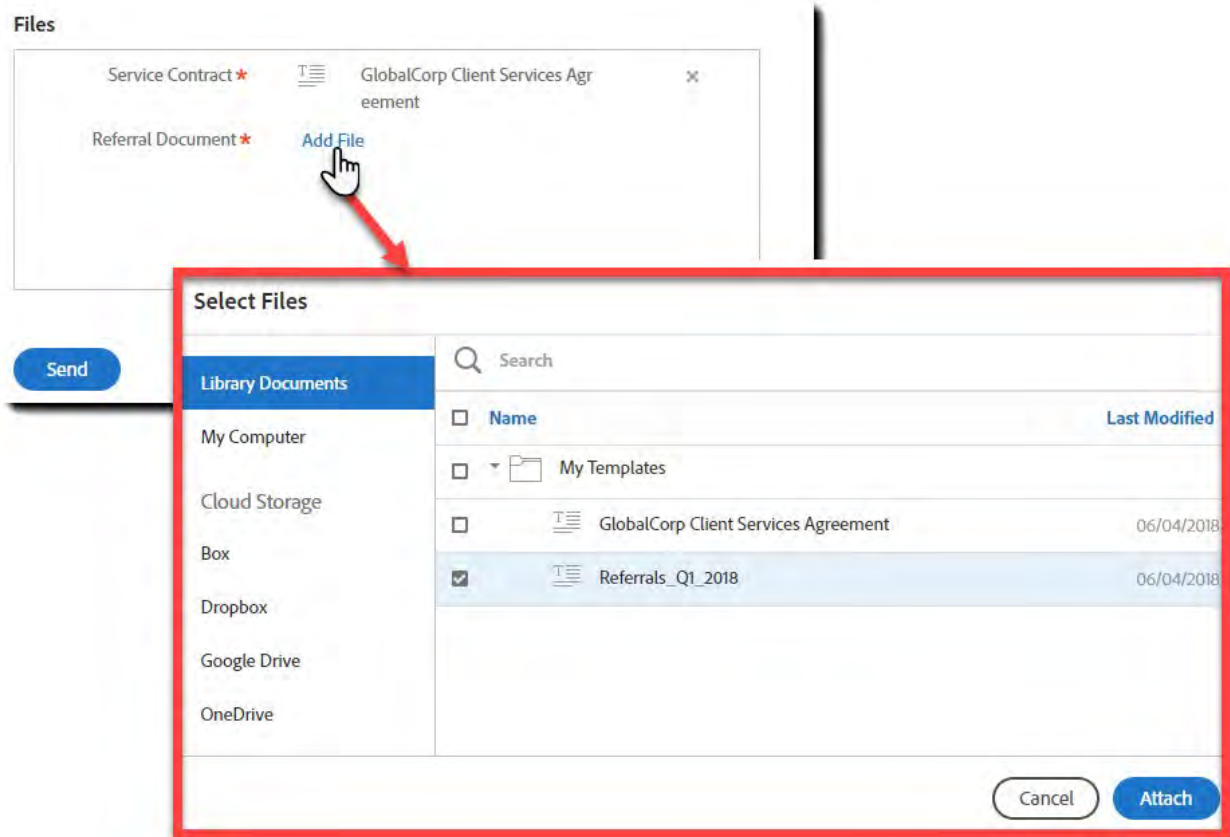
The recipient objects in the designer can now be marked as recipient groups. This allows the sender to configure an array of email addresses that are permitted to sign for that one signature step.

For example, if you need one of five managers to countersign, you can list all five emails, but only one needs to apply a signature.

The screenshot displays the Adobe Sign Workflow Designer interface. At the top, a 'Recipients Routing' diagram shows a sequence: 'Signer' (green person icon) → 'Counter Signature' (green person icon) → 'Legal team' (red person icon). Below this, the main workflow area is titled 'GlobalCorp Service Contract <50K'. It includes a description: 'How this workflow works? This workflow is used for contracts under 50K in addition to the service contract, the must include Bob, Carol, and Jane'. Under the 'Recipients' section, 'Signer*' is set to 'dave@caseyjones.com' and 'Counter Signature*' is set to 'Myself'. A 'Legal team*' section is highlighted with a red box, showing a list of recipients: 'Legal Team' (with a dropdown arrow), 'Bob@globalcorp.dom', 'Carol@globalcorp.dom', and 'Jane@globalcorp.dom'. To the right, a 'Legal team' configuration modal is open. It has an 'Email' field, a checkbox for 'This recipient is the sender' (unchecked), a checked checkbox for 'Mark as recipient group', a 'Role' dropdown set to 'Certified Recipient', checkboxes for 'Required' and 'Editable' (both checked), and an 'Identity Verification' section with 'Adobe Sign' checked and 'Phone' unchecked. A red arrow points from the 'Mark as recipient group' checkbox in the modal to the 'Legal team' section in the main workflow area.

File attachments

During the send process, documents can now be attached from any of the enabled Adobe Sign sources.



The user interface for the workflow send experience has been updated to a modern reflowable design, like the Send page.




The instructions that were previously to the right of the recipient list has been moved to the top of the page in a collapsible window.

GlobalCorp Service Contract <50K




How this workflow works?
This workflow is used for contracts under 50K. In addition to the service contract, the current referral sheet must be added. The legal recipient group must include Bob, Carol, and Jane.

Recipients ?



Signer *


  Phone 


Counter Signature *


  Adobe Sign 

Legal team *

 Adobe Sign

 Adobe Sign


 Adobe Sign

Document Name *





Options ?

☐ Set Reminder

Message *

Please find attached the service contract for 2018.
If you have any questions, don't hesitate to contact your account manager 

Files

Service Contract *		GlobalCorp Client Services Agreement	
Referral Document *		Referrals_Q1_2018	

Creating a custom workflow

Only administrators can create workflows. Account administrators can create workflows for their entire account or for specific groups within their account. Group administrators will be able to see all workflows, but can only edit the ones in their group.

Creating a workflow consists of defining the following information:

- **Workflow Info**—Define the workflow itself, which includes naming it, entering custom instructions for the senders using it, and granting permissions to use it.
- **Agreement Info**—Define and customize the agreement information that displays on the *Send* page.

- **Recipients**—Create a routing by adding recipients (signers and approvers) in the required signing order.
- **Emails** – Specify emails to be sent to different participants at different steps of the signature process.
- **Documents**—Specify which documents should be included in the workflow
- **Sender Input Fields**— Define fields that senders can use to input information when sending the agreement. The send input information is merged into the agreement before it is sent to the signers and approvers.

Required fields are identified with a red asterisk. Some field labels are editable as indicated by the pencil icon, for example Agreement Name:



Click the pencil icon to enter a custom label. This label will display on the Send page when the workflow is used to send a document. To revert back to the original label, click the revert icon.

- Workflow Info
- Agreement Info
- Recipients
- Emails
- Documents
- Sender Input Fields

Once the Workflow is fully configured, click **Save** at the top of the page.

To activate the workflow immediately, click **Activate**. The Workflow can be edited at any time.

Sending using a custom workflow

You can send an agreement using a workflow. When you select a workflow, the *Send* page displays the custom fields defined, including custom instructions, the default recipients and so forth.

- The Sending process


Signing and approving a workflow agreement

The workflow agreement is sent out in the order specified in the routing. The signers and approvers can sign using the link in the Please sign/Please approve email or from their Manage pages if they are registered Adobe Sign users. This works the same way as standard send process.

The history and audit report for the workflow agreement can be accessed from the Manage page. While the agreement is in process, you can add reminders and perform other tasks.

Editing a custom workflow

➤ [How to update existing Workflows](#)

 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)

**SIGN**

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe

 [Change region](#) ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

[Adobe Sign](#)

-
- [Sign In](#)

Adobe Sign REST API Version 6 Methods

Documentation for [Version 1](#), [Version 2](#), [Version 3](#), [Version 4](#), and [Version 5](#) is also available.

Introduction

Adobe Sign's REST API provides a powerful and easy way to integrate Adobe Sign functionality into your own applications. You can browse through the supported operations, categorized by the resources they apply to, in the [Resources and Operations](#) section below. You can even invoke the operations directly from this page using the corresponding "Try it out" functionality!

How to get started

1. Obtain a unique set of credentials (an ID and a secret) for use in your application. Account administrators can generate these credentials through the Adobe Sign API page in the account settings.
2. API calls require an [OAuth Access Token](#). Each operation on a resource requires specific OAuth scope(s), and your application will need to request all of the needed scopes during the OAuth authorization process.
3. Use this OAuth access token in the following REST endpoints to perform operations on behalf of the user who authorized the API access.

Note that from version 5 onwards, the API calls listed below **must** be made on a specific base URL obtained either using the OAuth workflow (the `api_access_point` parameter that is included with an authorization code) or by making a call to the `GET /baseUri` endpoint. Calls made on the wrong access point will return a 403 status code specifying `INVALID_API_ACCESS_POINT` as the reason. The `GET /baseUri` endpoint itself can be called on <https://api.echosign.com/api/rest/v6>. To learn more, please refer the [Getting Started Guide](#).

Using the "Try it out" functionality

To use the "Try it out" functionality applicable to each operation, first provide valid values for each parameter under the "Value" column. To easily populate complex parameter values, select "Model Schema" under the "Data Type" column and then click on the JSON text that is revealed. You can then edit the populated "Value" field as needed, and click the corresponding "Try it out" button to watch the API operation in action.

Developer Implementation Notes

1. Some API endpoints return identifiers or URLs that can be used in subsequent calls. While the API does not specify how long these identifiers or URLs can be, in practice developers should design their applications to handle up to 2083 characters for URLs and 512 characters for the identifiers.
2. New enum values can be added in future to an enum set in request and response for the same version of API. API clients should be prepared to handle additional values in every enum set and handle such cases of additional values in a manner that would be appropriate for their workflow. Example: If a new status for Agreement comes in future, client could ignore agreements with status that it does not

- [Creates a participantSet to which the agreement is forwarded for taking appropriate action.](#)
- [post /agreements/{agreementId}/members/share](#)
 - [Share an agreement with someone.](#)
- [post /agreements/{agreementId}/reminders](#)
 - [Creates a reminder on the specified participants of an agreement identified by agreementId in the path.](#)
- [post /agreements/{agreementId}/views](#)
 - [Retrieves the latest state view url of agreement.](#)
- [get /agreements](#)
 - [Retrieves agreements for the user.](#)

OAUTH ACCESS-TOKEN

Parameters

Parameter	Value	Description	Specify As	Data Type
Authorization	<div style="border: 1px solid black; padding: 2px;">(required)</div>	An OAuth Access Token with scopes: <ul style="list-style-type: none"> ▪ agreement read in the format ' Bearer {accessToken} '. The userId or email of API caller using the account or group token in the format	header	string
x-api-user	<div style="border: 1px solid black; padding: 2px;"></div>	userid:{userId} OR email:{email} . If it is not specified, then the caller is inferred from the token. The userId or email in the format userid:{userId} OR email:{email} .	header	string
x-on-behalf-of-user	<div style="border: 1px solid black; padding: 2px;"></div>	of the user that has shared his/her account	header	string

Parameter	Value	Description	Specify As	Data Type
externalId	<input type="text"/>	Case-sensitive ExternalID for which you would like to retrieve agreement information. ExternalId is passed in the call to the agreement creation API	query	string
showHiddenAgreements	<input type="checkbox"/>	A query parameter to fetch all the hidden agreements along with the visible agreements.	query	boolean
cursor	<input type="text"/>	Used to navigate through the pages. If not provided, returns the first page.	query	string
pageSize	<input type="text"/>	Number of intended items in the response page.	query	integer

Response Class

- [Model](#)
- [Model Schema](#)
- ⊕ ... [UserAgreements {](#)

Accept: **application/json**

Error Status Codes

⊕ ... [show](#)

Try it out!

- [get /agreements/{agreementId}](#)
 - [Retrieves the current status of an agreement.](#)
- [get /agreements/{agreementId}/auditTrail](#)
 - [Retrieves the audit trail of an agreement identified by agreementId.](#)

Field types

[Search Adobe Support](#)[Sign In](#)

Search



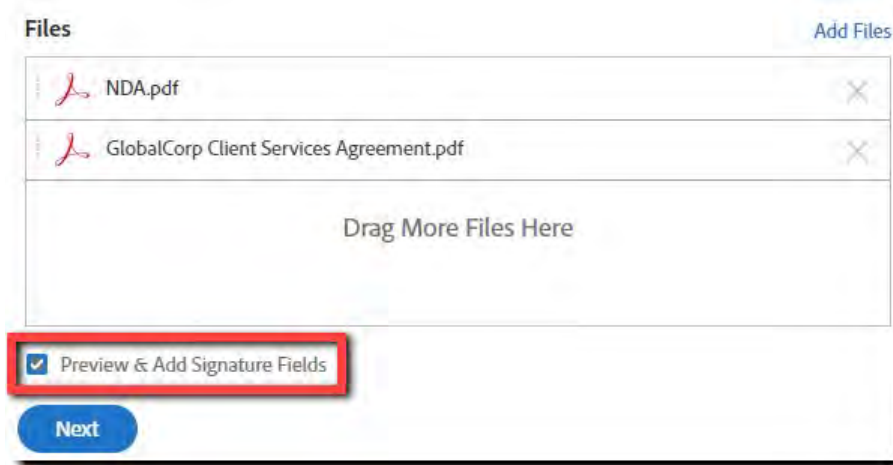
SIGN ▾

Agreement field types

Agreement fields can contain various data. You can determine what type of data can be entered into a field by defining the field type. Adobe Sign has various field types that can be placed on a document. These field types can obtain certain data such as signatures, initials, company, or job title. You can also create a field and customize what type of data can be entered (such as Phone number, or credit card number).

Tick the check box **Preview & Add Signature Fields** to launch the Drag & Drop Authoring tool. With this tool, fields can be placed on your document. Enable this check box:

- on the Send page when sending an agreement
- when creating a library document or template
- when creating a widget



Field-level field type selection

Within the properties of most field types, there is a drop down value that allows you to change the type of field to any other field type.

This will significantly speed up form creation when used in conjunction with [Automatic Field Detection](#).

Signature Approvals

Client

GlobalCorp

Digital Signature

Signature

Name

Title

Date

Digital Signature 1

Assigned To Participant 1

Field Type

- Digital Signature
- Signature Fields
 - Signature
 - Digital Signature**
 - Initials
 - Signature Block
- Signer Info Fields
 - Title
 - Company
 - Name
 - Email
 - Date
- Data Fields
 - Text Input

Signature fields

Signature

Digital Signature

Initials

Signature: **Signer Name (Date)**

Email:

Stamp

W: 3.5 cm
H: 3.5 cm

Signature Fields

- Signature
- Digital Signature
- Initials
- Signature Block
- Stamp

Signer Info Fields

Data Fields

More Fields

➤ Signature block

➤ Stamp

Signer info fields



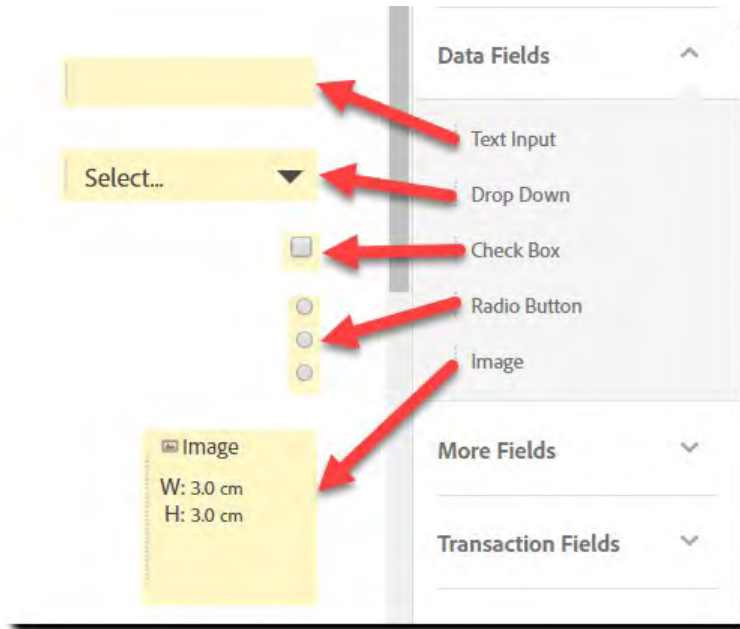
Signer info fields are used to collect specific information stored in Adobe Sign. Registered users have this information under their profile.

Usually, these fields are automatically populated with the information on record for the assigned user.

➤ Title and Company

➤ Signer name, e-mail, and date

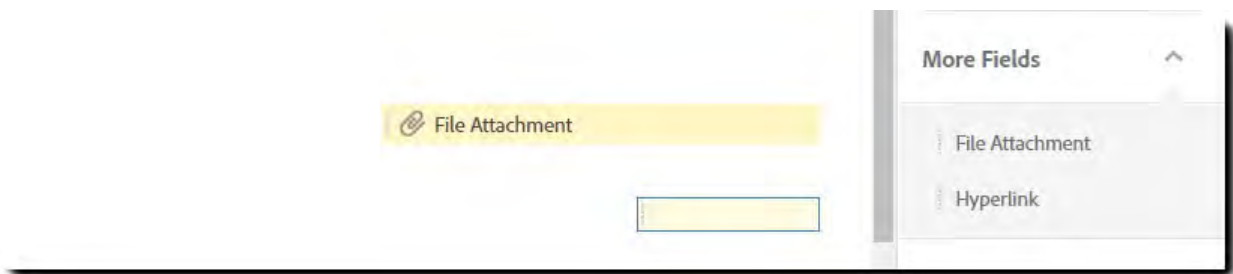
Data fields



Data fields are used to collect additional information from the recipient. It also includes objects the recipient can use to make selections or choose options.

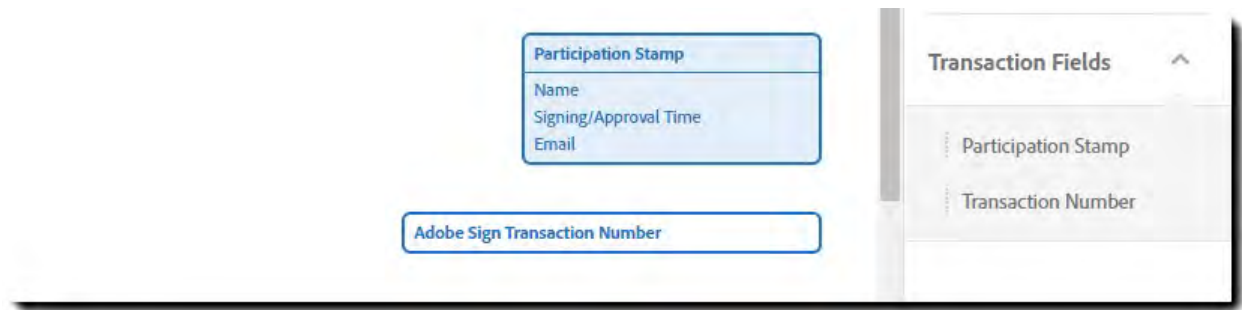
- Text field
- Drop down
- Checkboxes and radio buttons
- Images

More fields




- File attachment
- Hyperlink

Transaction Fields



➤ Participation Stamp

➤ Transaction Number

 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [AdChoices](#)

Set reminders



Search Adobe Support



Sign In

Search



SIGN

Set a reminder for a transaction

Reminders are just that. They're used to remind signers they have a document that is waiting for them. They are sent in the form of emails and can be sent at certain intervals.

▼ Setting a reminder when the transaction is sent

- 1 You can set a reminder for the transaction directly on the Send page, in the lower right section, just to the right of the *Message* field.

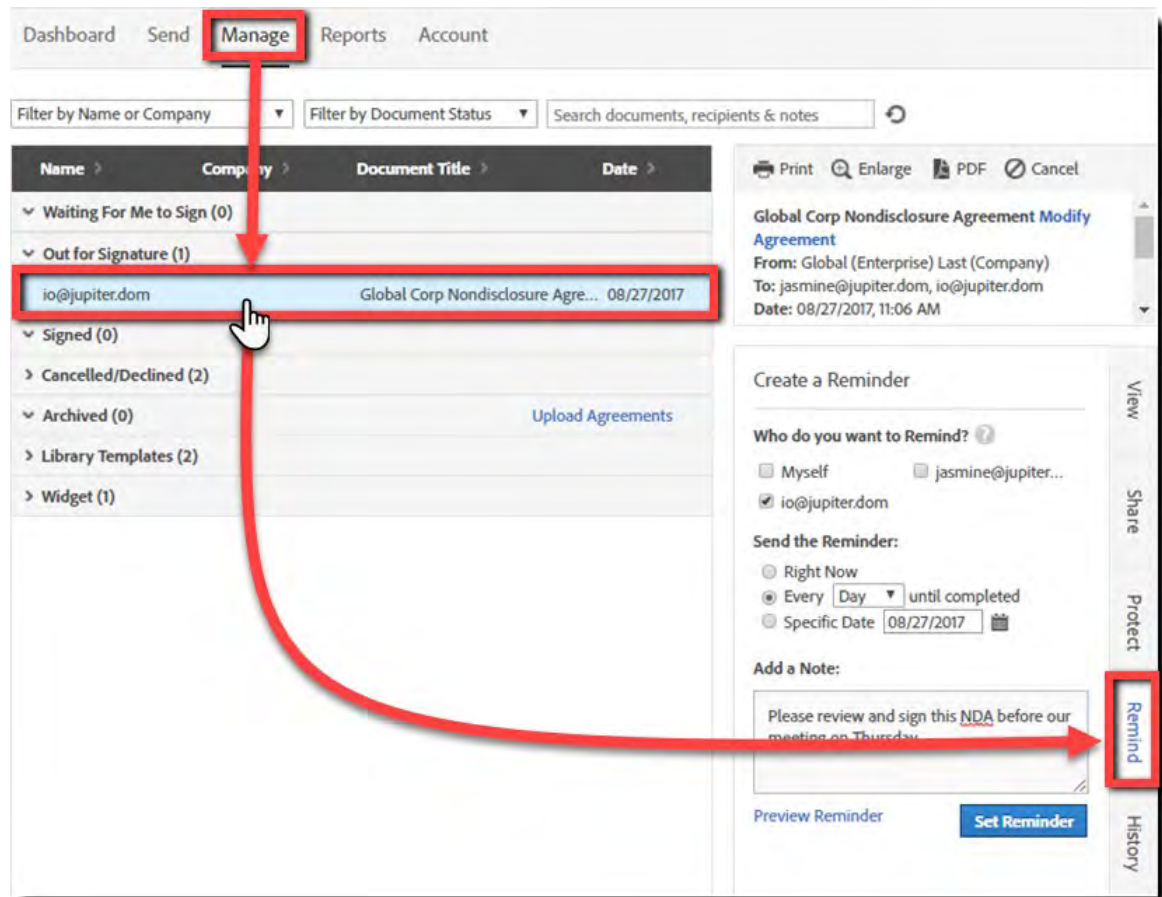
Check the **Set Reminder** box to open the options

The screenshot shows the Adobe Sign 'Send' page. At the top, there are tabs for 'Dashboard', 'Send', 'Manage', 'Reports', and 'Account'. The 'Send' tab is active. Below the tabs, there's a 'Recipients' section with a toggle for 'Complete In Order' and a link to 'Add Recipient Group'. A list of recipients is shown, with the first one being 'jupiter@jupiter.dom'. Below the recipients, there's a 'Message' section with a text area containing 'Agreement Name' and 'Please review and complete this document.' To the right of the message, there's an 'Options' section. In the 'Options' section, the 'Set Reminder' checkbox is checked, and the frequency is set to 'Daily'. The 'Options' section also includes checkboxes for 'Password Protect' and 'Completion Deadline'. The 'Set Reminder' section is highlighted with a red box.

- 2 Set how often you would like the reminder to be sent (daily or weekly). Reminders will be sent on the chosen iteration using the time stamp value for when the agreement was sent.

▼ Set a reminder on a transaction that was already sent

- 1 As the sender of the agreement, go to the **Manage** page, single-click the agreement and click the **Remind** tab on the right side of the page.



- 2 In the information window, check who you want to remind, the frequency of the reminder and a note to send in the reminder email. Once you've set it up, click the **Set Reminder** button.

Create a Reminder

Who do you want to Remind? ⓘ

☐ Myself ☐ jasmine@jupiter...

☒ io@jupiter.dom

Send the Reminder:

☐ Right Now

☒ Every until completed

☐ Specific Date ⓘ

Add a Note:

Please review and sign this NDA before our meeting on Thursday.

[Preview Reminder](#) [Set Reminder](#)

View Share Protect Remind History

A success banner will appear at the top of the screen after the reminder is created.

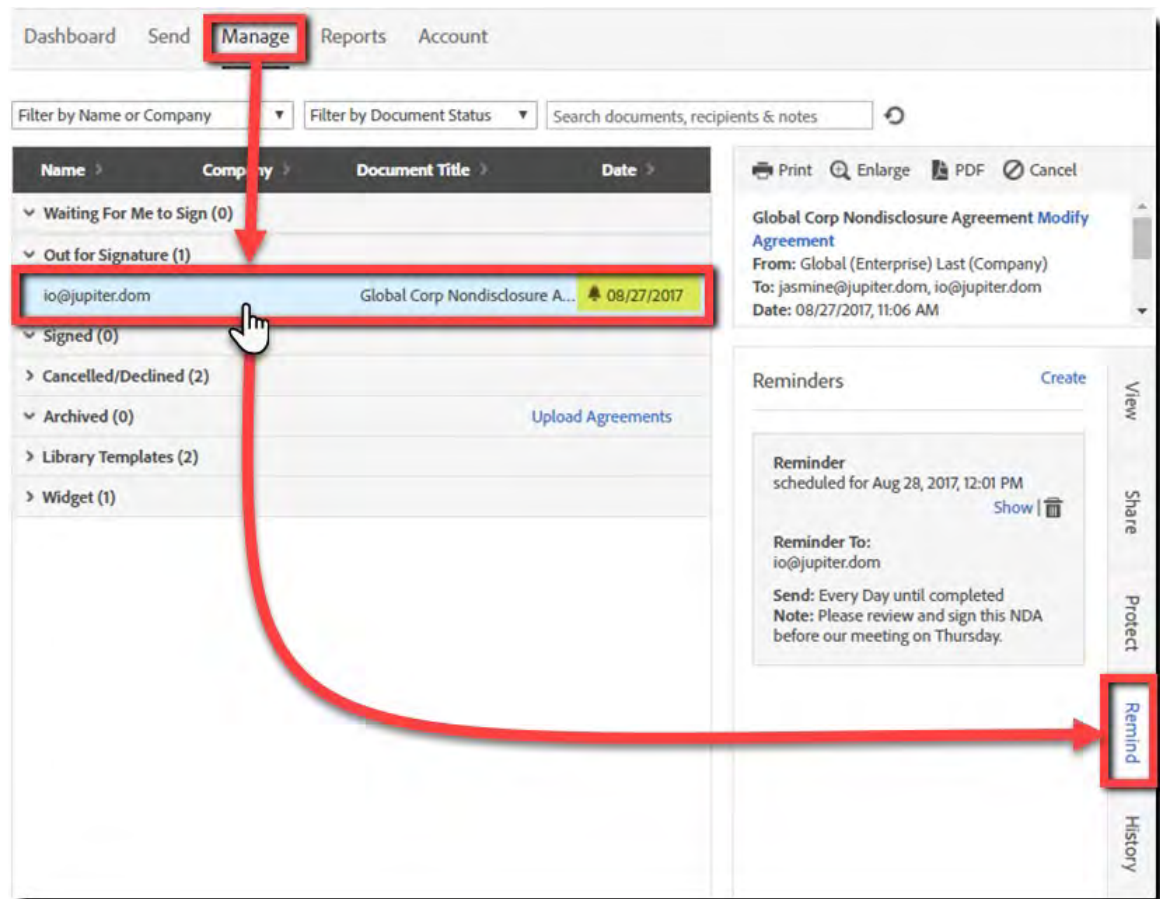
Dashboard Send **Manage** Reports Account

A reminder will be sent to io@jupiter.dom.

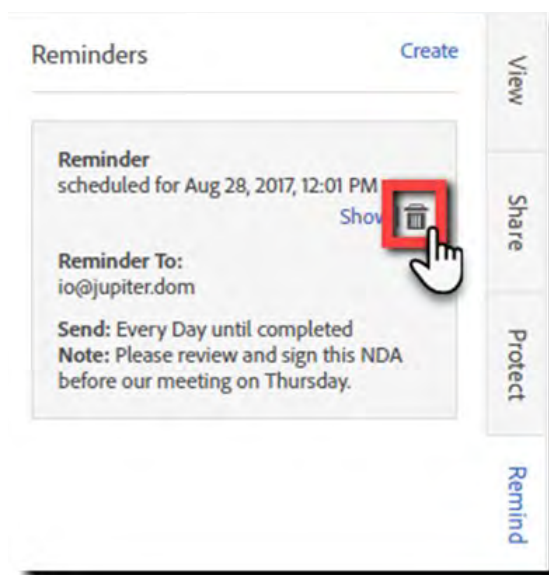
Filter by Name or Company ▼ Filter by Document Status ▼ Search documents, recipients & notes ⓘ

▼ Cancel a reminder

- 1 As the sender of the agreement, go to the **Manage** page, single-click an agreement with the reminder icon, and click the **Remind** tab.



- 2 In the information window, click the **Trash Can** icon. The reminder is canceled for the whole transaction.





Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

[Sign In](#)

Adobe Support policies: Service level agreements

Gold support

Search Adobe Support

ON THIS PAGE



Search

Target response times#

Hours of availability*

(During normal business hours by region)

- 24x7 support, 365 days per year

- **Priority 1:** 30 minutes
- **Priority 2:** 1 hour
- **Priority 3:** 4 hours
- **Priority 4:** 1 business day

[Find out more about priority definitions](#)

[Gold support](#)

[Platinum maintenance and support](#)

[Enterprise support for Creative Cloud, Document Cloud, Digital Publishing Suite](#)

[Technical solution management](#)

[Case priority definitions](#)

Last Published: **April 10, 2018**

Platinum maintenance and support

Target response times#

Hours of availability*

(During normal business hours by region)

- 24x7 support, 365 days per year

- **Priority 1:** 30 minutes
- **Priority 2:** 1 hour
- **Priority 3:** 4 hours
- **Priority 4:** 1 business day

[Find out more about priority definitions](#)

Enterprise support for Creative Cloud, Document Cloud, Digital Publishing Suite

Target response times#

(During normal business hours by region)

- **Priority 1:** 30 minutes
- **Priority 2:** 1 hour
- **Priority 3:** 4 hours
- **Priority 4:** 1 business day

[Find out more about priority definitions](#)

[Find out more about Enterprise Support](#)

Hours of availability*

- 24x7 support, 365 days per year

Technical solution management

Target response times#

(During normal business hours by region)

- **Priority 1:** 30 minutes
- **Priority 2:** 1 business hour
- **Priority 3:** 2 business hours
- **Priority 4:** 1 business day

[Find out more about priority definitions](#)

Hours of availability*

- 24x7 support, 365 days per year

Case priority definitions

For the Enterprise Support, Platinum Maintenance and Support and Gold Support programs, it is you, the customer who identifies the priority level. Accurately prioritizing your technical issue is critical to our mutual success and the following guidelines will assist you in determining the appropriate priority level.

- **CRITICAL (Priority 1) — the problem results in extremely serious interruptions to a production system.** It has affected, or could affect, the entire user community. Tasks that should be executed immediately cannot be executed because of a complete crash of the system or interruptions in main functions of the production system. Data integrity is compromised and the service request requires immediate processing as the issue can result in financial losses. In a desktop application, whether part of, or independent of a solution, the issue is at risk of creating imminent financial losses due to missing critical project deadlines or deliverables. The customer shall call Adobe Customer Support for all critical priority 1 issues.
- **URGENT (Priority 2) — the problem results in serious interruptions to normal operations, will negatively impact an enterprise-wide installation, urgent deadlines or at risk.** In a production system, important tasks cannot be performed, but the error does not impair essential operations. Processing can still continue in a restricted manner, and data integrity may be at risk. In a pre-production environment, the problem hinders deployment of an enterprise installation. In a desktop application, meeting urgent project deadlines that have a financial impact are at risk. The service request requires timely processing, because the malfunction could cause serious interruptions to critical processes or negatively impact business.

- **IMPORTANT (Priority 3) — the problem causes interruptions in normal operations.** It does not prevent operation of a production system, or there could be minor degradation in performance. The error is attributed to malfunctioning or incorrect behavior of the software. The issue will affect a pilot or proof-of-concept deadline in a development environment. In a desktop application, meeting important project deadlines may be at risk.
 - **MINOR (Priority 4) — the problem results in minimal or no interruptions to normal operations** (no business impact). The issue consists of "how to" questions including issues related to APIs and integration, installation and configuration inquiries, enhancement requests, or documentation questions.
-

NOTE

Mission-critical support is provided by telephone 24 hours a day, 7 days a week, 365 days a year for Priority 1 issues. Non-critical issues are responded to during standard regional business hours.

* Denotes case intake coverage.



Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)

[^ Back to top](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)



Sign In



SIGN ▾

Reporting

Search Adobe Support



Search

Create a report

Adobe Document Cloud for enterprise - Premium accounts, can run a report on transactions sent from users in the account. The report produces various graphs showing the signature percentage and the average time to sign. You can also export a CSV file with the raw data generated from the report.

Applies to: Sign

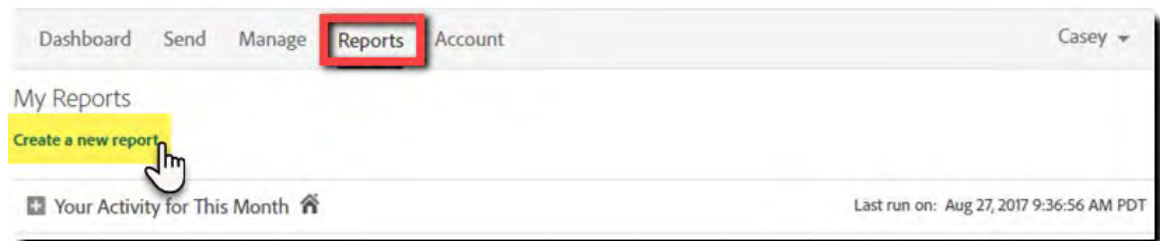
Last Published: August 27, 2017

▼ Quick steps

1. Click **Reports**.
2. Click **Create New Report**.
3. Set parameters for report (see third section).
4. Click **Run Report**.

▼ Step-by-step

- 1 To generate a report, click the **Report** tab, then click **Create a New Report**.



- 2 Set the various parameters to affect the resulting report and click **Run Report**. You can find account parameters in the next section.

Dashboard Send Manage **Reports** Account Casey ▾

Create a New Report

Creation Date ☐ This Week ☒ Last Week ☐ This Month ☐ Last Month ☐ Date Range

Users & Groups ☒ All Users ☐ Filter by User ☐ Filter by Group

Documents ☒ All Documents ☐ Filter by document

Document Name

Mega Sign ☐ Include MegaSign Agreements

Performance Goals Set your performance goals by specifying thresholds for gauge colors:

% Completed:	Green: > <input type="text" value="50"/> %	Yellow: > <input type="text" value="25"/> %
Time to Complete:	Green: < <input type="text" value="60"/> Min.	Yellow: < <input type="text" value="90"/> Min.

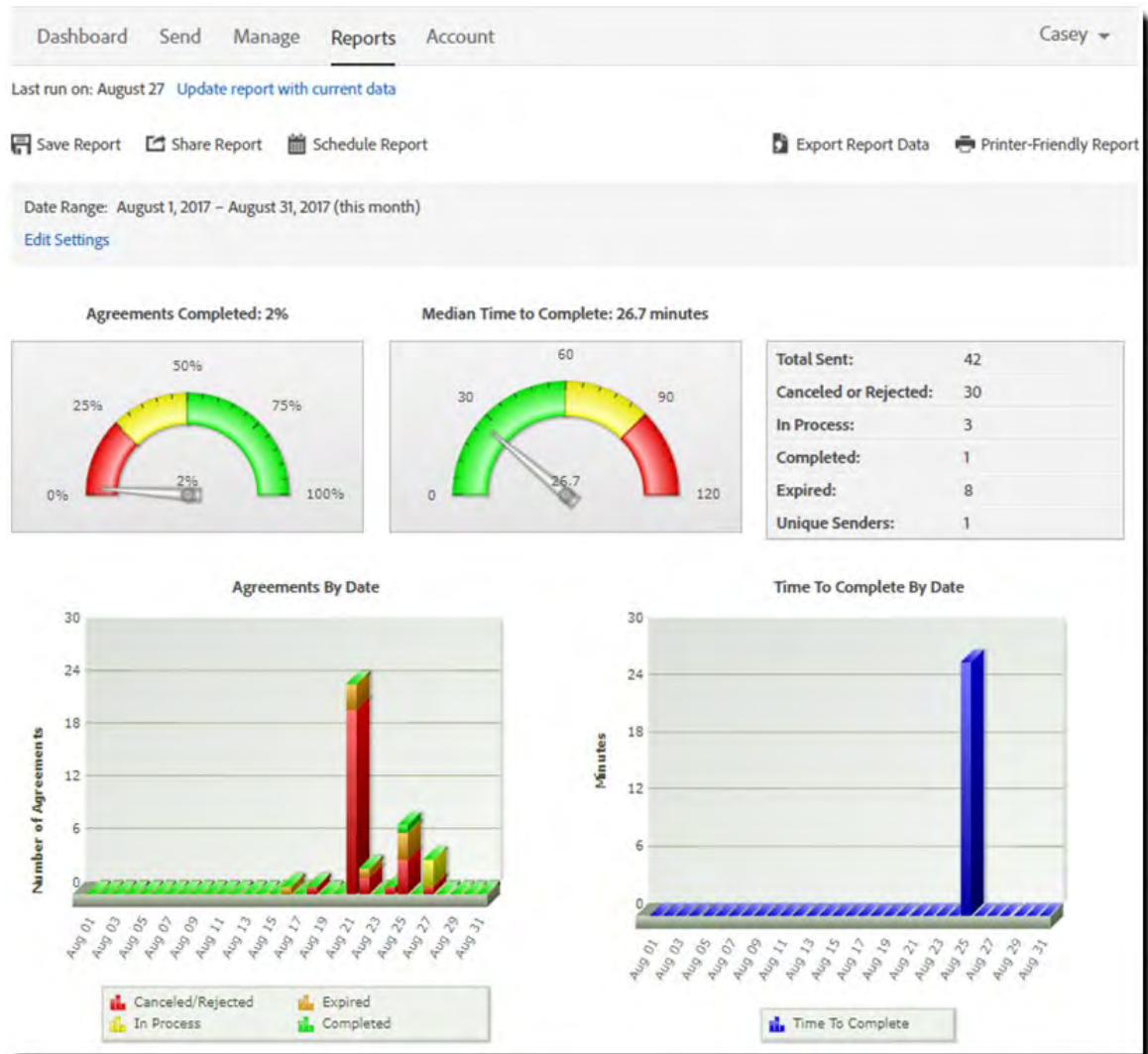
Benchmark Benchmarking is not enabled for your account. You can opt-in and enable it on the [report settings](#) page.

Graph Agreements By ☒ Date ☐ Sender ☒ Form ☒ Signature Type

Et Cetera Animation: ☒ Yes ☐ No Color Shading: ☒ Yes ☐ No Bar Charts: ☒ 3D ☐ 2D

Run Report Cancel

- 3 The report results page opens, displaying the information based on your parameters.



▼ Report parameters

Interval

The Interval section allows you to collect data from predefined time frames or a custom date range.

Interval ☐ This Week ☐ Last Week ☐ This Month ☐ Last Month ☒ Date Range

From to

June, 2014

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Select date

Users & groups

Users & Groups allows you to choose specific users or groups to collect information from.

Users & Groups ☐ All Users ☒ Filter by User ☐ Filter by Group

Garth Skjeggstad (hogarth.skjeggstad+1@g...
Hogarth Skjeggstad (hogarth.skjeggstad@...
hogarth.skjeggstad+new@gmail.com

Add Selected

Remove Selected

hogarth.skjeggstad+2@gmail.com

Documents

The documents area allows you to specify certain library documents that have been sent out.

Documents ☐ All Documents ☒ Filter by document

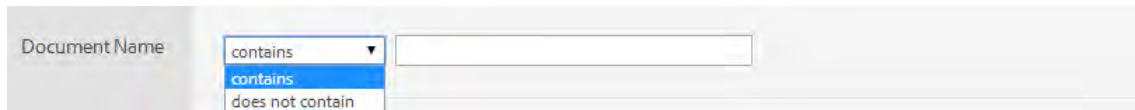
I-9 (Employment Eligibility Verification)
Other Users Test Template
Test Library Document
Test Library Document
W-4 (IRS Employee Withholding Allowance)
W-9 (Request for Taxpayer Identification Nu

Add Selected

Remove Selected

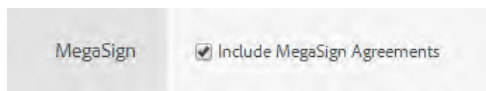
Document name

This option allows you to include parts of the document name in the report search.

A screenshot of a search filter interface. On the left, the text 'Document Name' is displayed. To its right is a dropdown menu with three options: 'contains' (selected), 'contains', and 'does not contain'. Further to the right is an empty text input field for specifying search criteria.

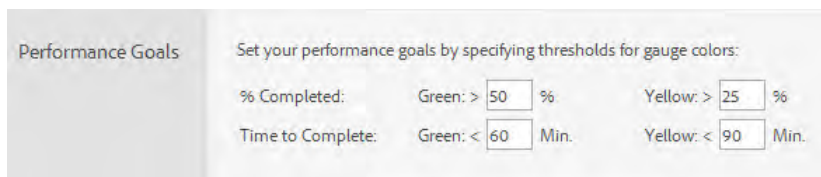
Mega Sign

Select this option if you want to include Mega Sign transactions in your report.

A screenshot of a toggle switch labeled 'MegaSign'. The switch is currently turned on, indicated by a checked checkbox and the text 'Include MegaSign Agreements'.

Miscellaneous report data

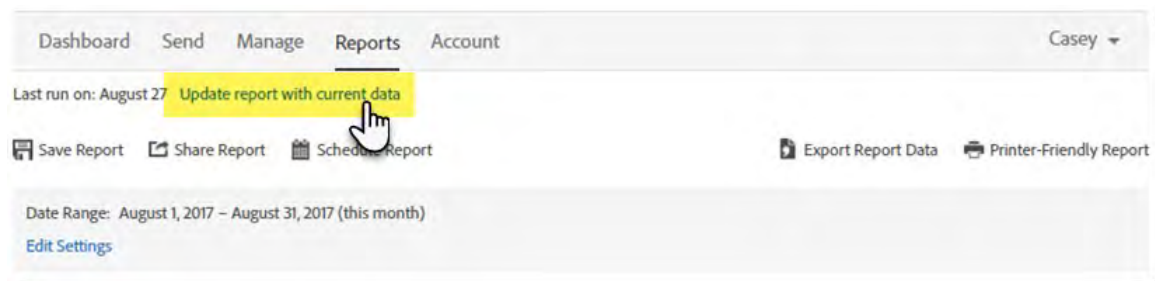
The last four settings found on the page are to change or visually alter the resulting report and related graphs.

A screenshot of the 'Performance Goals' settings section. It includes a header 'Set your performance goals by specifying thresholds for gauge colors:'. Below this are four input fields: '% Completed: Green: > 50 %', '% Completed: Yellow: > 25 %', 'Time to Complete: Green: < 60 Min.', and 'Time to Complete: Yellow: < 90 Min.'.

▼ Report data and options

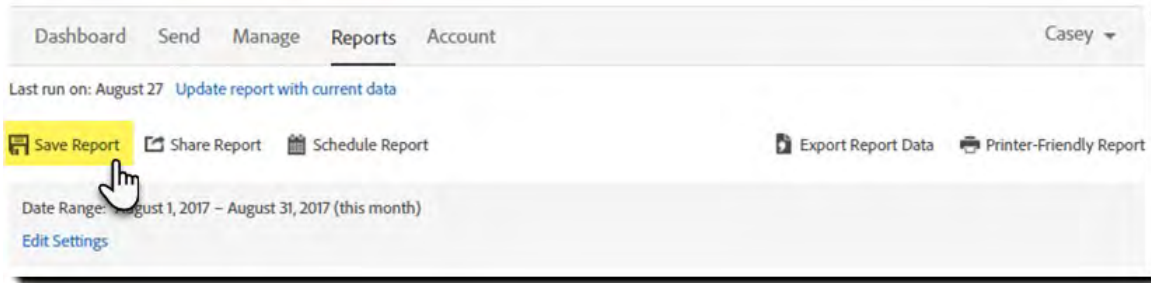
Update report with current data

This link refreshes the report to include recent transactions.

A screenshot of the 'Reports' tab in the Adobe Sign interface. The 'Reports' tab is selected in the top navigation bar. Below the navigation bar, the text 'Last run on: August 27' is displayed. A yellow button labeled 'Update report with current data' is highlighted, with a hand cursor pointing to it. Below this button are three icons: 'Save Report', 'Share Report', and 'Schedule Report'. To the right of these icons are two more icons: 'Export Report Data' and 'Printer-Friendly Report'. At the bottom, the 'Date Range' is set to 'August 1, 2017 – August 31, 2017 (this month)', and there is a link to 'Edit Settings'.

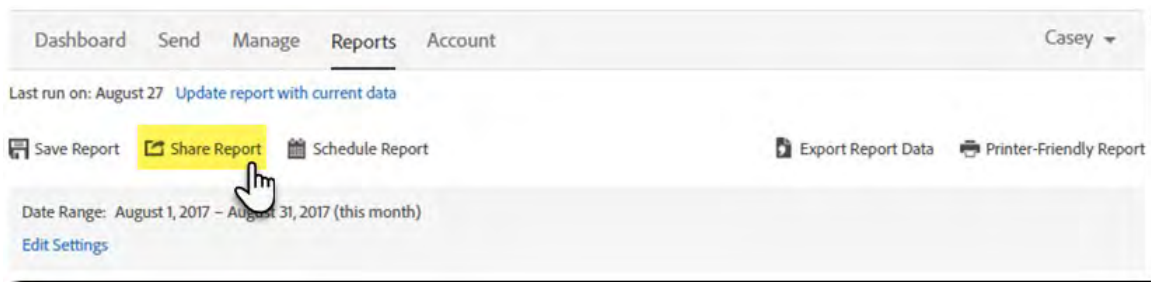
Save Report

Save Report allows you to save this report. You can access it again by clicking the Reports tab.



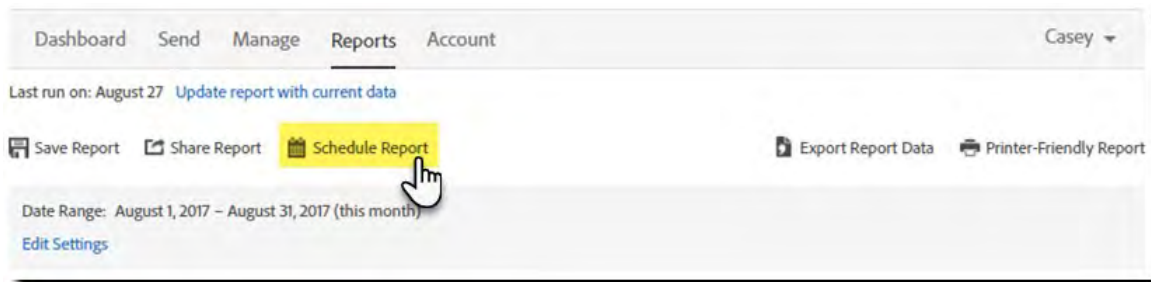
Share Report

This option allows you to share this specific report with an e-mail address and includes a custom message.



Schedule Report

Schedule Report uses the current report's settings to set up an automatic recurring report that is generated daily, weekly, or monthly. You can also choose the recipients that you want to send the recurring report to.

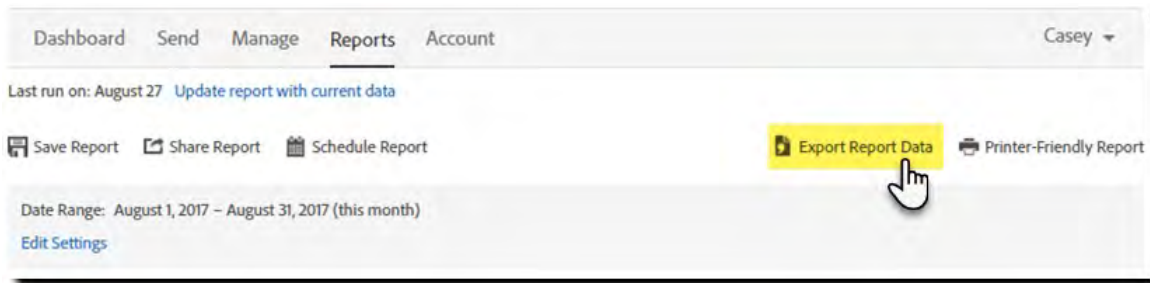


Export Report Data

Click Export Report Data to download a CSV file with the raw data generated in the report.

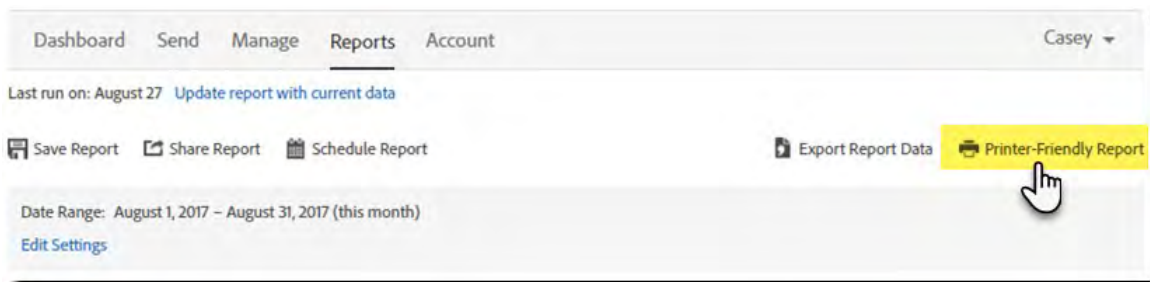
Note:


By default, field data is not contained in the report .CSV file. If you want to export the field data from signed agreements, the admin of your account needs to open a ticket with Support.



Printer-Friendly Report

Printer-Friendly Report serves up a version of the report with the various graphs removed and displays your report with just the numbers.



 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

[^ Back to top](#)

[Contact Us](#)

Ask the Community

[Ask now](#)

Post questions and get answers from experts.

Was this page helpful? ☐ Yes ☐ No

Products

Blogs & Community

Support

Adobe



Change region ▼

Copyright © 2018 Adobe Systems Incorporated. All rights reserved. / [Privacy](#) / [Terms of Use](#) / [Cookies](#) / [▶ AdChoices](#)

Adobe Document Cloud onboarding program

Ramp up quickly with onboarding services, included in your subscription



Adobe Document Cloud for enterprise includes onboarding services and continuing support to help you maximize the business benefits of electronic workflows. Jump-start your successful implementation by taking advantage of our expert guidance in onboarding.

Your subscription includes services to help you ramp up quickly and get the most out of your investment. Adobe's onboarding program provides personalized support to help you configure and customize your account as well as launch your initial use case. In partnership with your dedicated Customer Success Manager (CSM), an onboarding specialist will take the time to understand your business goals and work with you one-on-one to create and execute a deployment plan that's tailored to your organization.

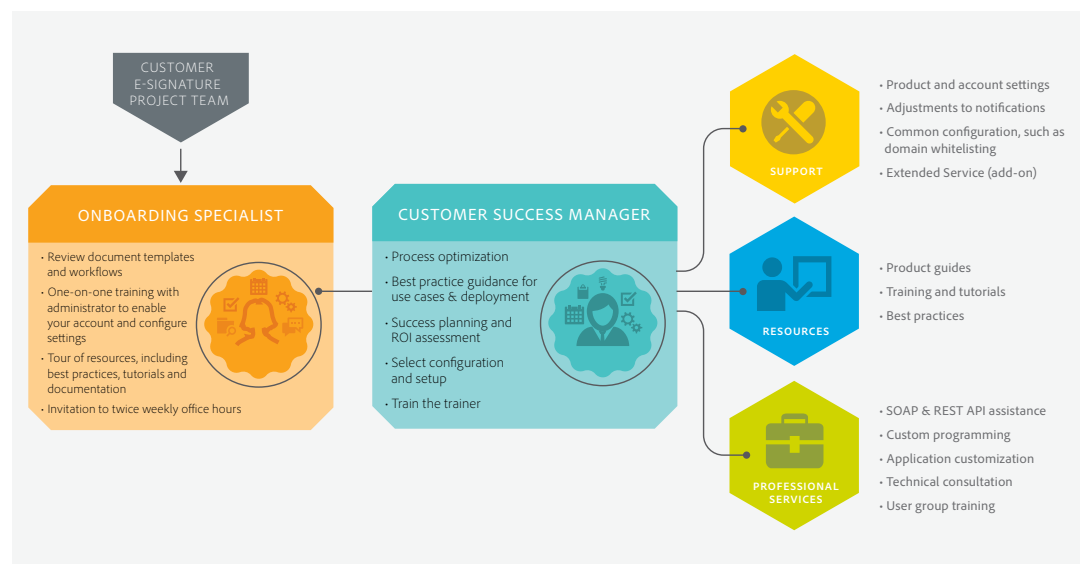
To put you on the road to success, we'll show you best practices and *Adobe Document Cloud* features and capabilities, including third-party integrations, as well as how to reach Adobe experts and extended support when needed. You'll also receive a wealth of resources such as twice weekly Ask the Experts office hours, training videos, best practice articles and newsletters to keep you informed and educated.

Faster ROI with onboarding services

Whether your goal is improving workforce productivity, speeding business processes, increasing customer satisfaction or meeting security and compliance objectives, we're here to help you get there. With onboarding support, thousands of customers just like you have started capturing *electronic signatures* without delay.

The first phase of onboarding is about enabling the account administrator. Your onboarding specialist will review your business goals and provide recommendations for workflows, document templates, document management procedures and reporting. The specialist will help you configure and customize your account as well as create a go-live plan to get you up and running quickly on your first use case.

Next, we'll provide resources to help you train your end users. End-user buy-in and education is a key component of successful deployments, and we recommend the following best practice guides for this phase: [Creating an effective deployment communication plan](#) and [5 steps to developing an effective training plan](#). We also offer additional group training through Adobe Professional Services.



The Adobe Document Cloud customer success ecosystem

Ongoing support from your CSM

The onboarding process is complete once your initial use case is deployed and you are transacting agreements through the new electronic workflow. Your CSM has been with you from day one and at this point becomes your primary adviser and point of contact for the life of your subscription. As you begin to refine and extend *e-signatures* into additional workflows and use cases, your CSM will ensure you have the resources and support you need to be successful. That includes helping you set and achieve new goals—your CSM will help you define KPIs and will track and review your progress at each milestone.

Extended support and services

Sometimes customers require additional support to fast-track deployment, bring different teams up to speed or implement custom documents, workflows or integrations. Adobe Professional Services is available to help. Learn more about our paid [Professional Services](#) for technical consulting, development and end-user training.

Resources

- [Adobe Document Cloud Customer Success datasheet](#)
- [Adobe Professional Services for Adobe Sign datasheet](#)
- [Implementing Adobe Sign, a best practices guide](#)
- [Creating an Effective Deployment Strategy for Adobe Sign](#)
- [5 steps to developing an effective training plan](#)
- [Creating an effective deployment communication plan](#)





Access a world of support from a single point of contact.

Lean on your Customer Success Manager to help you drive ROI.

With Adobe Document Cloud, you get more than all-digital, end-to-end document workflows. You will have a team of Adobe resources to help you get the very best return on your investment, starting with your Customer Success Manager (CSM).

Think of your CSM as a trusted advisor who will work with you to understand the unique needs of your enterprise, then connect you with the people, information, and resources you'll need to start strong and find long-term success.

"The support from the Adobe team during the pilot and implementation phases has been instrumental in our overall success."

JARROD KINGSTON

Business Systems Manager
Penton

Trust your CSM to take you where you need to go.

Throughout the term of your agreement, your CSM will be there to make sure you accomplish all of your Adobe Document Cloud goals, no matter what they might be. They'll help you identify KPIs, develop an action plan to reach them, and track your progress along the way. They'll also help you schedule time with Adobe Expert Services, Support, and any other Adobe resources you'll need to ensure your company's success.

Your CSM connects you with the right people and the right tools at the right time.

Resources

Get product guides, training materials, tutorials, and best practices for use case deployments.

Professional Services

Meet with Adobe experts who will provide technical consultations on integrations and custom workflows.



Support

Ask any question or raise any issue, the Customer Care team will answer.

Onboarding Specialist

Set up product and account settings, and receive Admin and User training.

Deploy with confidence.

Your onboarding specialist and CSM partner to make your launch and ongoing deployments successful. Onboarding assists with account set-up, and administrator and user training. Our specialist will also connect you with extensive Adobe resources and ensure the successful deployment of your first use case.

Immediately following, your CSM will take the lead in helping you with the digital transformation of your business. As an Adobe Document Cloud subscriber, you'll have access to best practices and receive guidance in use case deployment. Further trainings and online resources are also available.

Your CSM is your connection to our Customer Care team and Adobe Professional Services. Customer Care experts can address product issues or questions, like whitelisting or adjusting notifications, and help you maintain Adobe applications as your solution evolves. Adobe Professional Services provides a range of expertise, including how to use our APIs, design guidance, and custom solutions.

Set the right course and stay on track.

Once your first use case has been launched, your onboarding will be complete, and your CSM will become your primary advisor and point of contact. Together, you'll determine what goals you'd like to achieve with Adobe Document Cloud—like better operational efficiencies or saving money—and develop a Success Plan that will help you reach them. Each month, your CSM will meet with you to review the KPIs you set in your Success Plan, assess your progress toward meeting them, and if necessary, discuss strategies for improvement.

In addition to monthly meetings, your CSM will schedule a quarterly Executive Business Review to discuss how your teams are using Adobe Document Cloud, and point out untapped potential. They'll also provide updates on the latest feature rollouts, product roadmaps, and future digital transformation opportunities.

On each anniversary, your CSM will arrange for you and your Account Executive to review together your journey as an Adobe Document Cloud subscriber. And at the end of your subscription term, your CSM will work with you to help you plan for your future document solution needs.

"The ongoing support from Adobe has been exceptional, which helps us address our business needs today and into the future."

JOOST VAN DE BUNT

Business Development Manager
KLM

Discover a partner who stands beside you all the way.

All-digital document workflows give you the power to improve workforce productivity, speed business processes, and increase customer satisfaction. With Adobe Document Cloud, you get all that, and a CSM to help guide you through every process, and every decision.

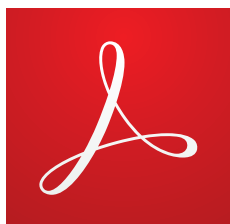
To learn more, contact your CSM or your Adobe sales representative.

Get support at every step.

- Immediate onboarding
- Weekly status meetings during onboarding
- Quarterly executive business reviews
- Anniversary status reviews

Adobe Professional Services for Adobe Sign

Partner with Adobe Experts to shorten time to value



"The service and partnership with the Adobe team has provided significant advantages to our strategy overall. Within a week, we had a fully functioning Adobe Sign trial, and sales personnel were already trained and using the product. The merits of Adobe Sign were clear to us. Our culture definitely aligned with Adobe's culture."

Brett Orr,
Head of Service Delivery,
reed.co.uk

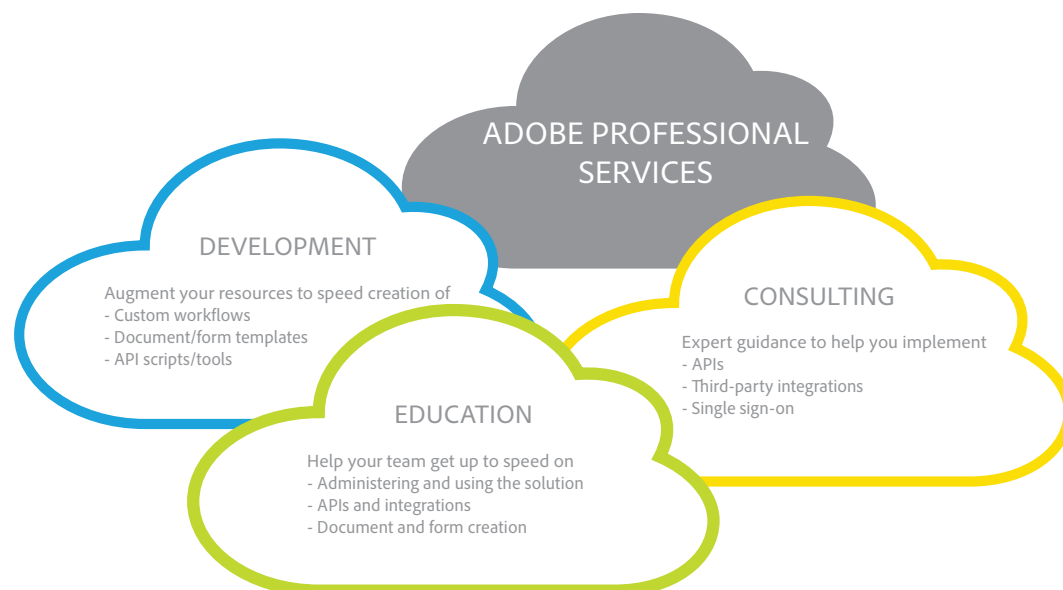
Partner with Adobe Professional Services to maximize your investment in *Adobe Sign*, an *Adobe Document Cloud* solution. Our qualified solution architects can help you create, develop, deploy, customize and optimize your implementation to help ensure success.

You've purchased Adobe Sign and are excited about the benefits it can bring to your customers and organization. However, you may need help bringing different teams up to speed, deciding on the best way forward or implementing custom documents, workflows or integrations. Adobe Professional Services experts can help make the most of your investment.

Accelerate time to value with Adobe Sign

Adobe Professional Services enhances your expertise and resources, so you can start generating value sooner from your Adobe Sign investment. Services fall into three categories that you can combine to suit the needs of your organization:

- **Consulting:** Receive technical advice on how to best configure, integrate and expand the use of Adobe Sign in your environment.
- **Development:** Extend your development team with experts to shorten delivery times.
- **Education:** Develop your team's skills and gain greater control of your implementation.



Engage easily with Adobe Professional Services

Understanding your needs and challenges is the first step on our path to mutual success. Each Adobe Professional Services project begins with a key stakeholder meeting to develop a comprehensive description of necessary requirements that inform the statement of work (SOW). The SOW describes the proposed solution and the process for managing changes and billing. Once you have approved the final SOW, a schedule is set and work begins.

Take advantage of packages for popular services

Adobe Professional Services has created packages for the most frequently requested services. If you don't see the service you need, just ask—we've likely done it before and can provide cost estimates. Adobe Professional Services work is billed at US\$250 an hour, plus travel expenses if necessary.

Most requested packages	Description
Consulting services	
Salesforce	Setup and configuration assistance for Adobe Sign with Salesforce objects, data mapping, custom triggers and workflows
Microsoft Dynamics	Setup and configuration assistance for Adobe Sign with Microsoft Dynamics entities
SharePoint	Setup and configuration assistance for Adobe Sign with Microsoft SharePoint
SAML	Expert advice on implementing Adobe Sign within your single sign-on (SSO) environment
Adobe Sign API integration	A review of the Adobe Sign architecture and APIs, integration best practices and answers to technical implementation questions
Development services	
Custom workflows	Customization of the Send feature to work with your business processes
Document/form creation	Template or document creation with form and signature fields, field validation and conditional logic
Custom API scripts/tools	Script development to automate tasks
Salesforce QS	Installation of the Adobe Sign managed package and creation of Salesforce triggers, workflows, Visualforce pages and more
Account administration	Expert administration of your Adobe Sign account
Education services	
User/administrator	Customized training using your documents and workflows
Documents/forms	Instruction on creating professional documents and intelligent forms
Adobe Sign API	Instruction on using REST or SOAP APIs

Contact your Account Executive or Customer Success Manager for more information.



Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2016 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

Extended Service offering for Adobe Document Cloud eSign services

Personalized service with the highest level of responsiveness and expertise.



Is the Extended Service offering for me?

The Extended Service customer care offering is designed for Document Cloud eSign services customers that:

- Have invested in Adobe products for mission-critical business needs
- Are seeking a more hands-on, personalized relationship with Adobe for expertise in a complex environment
- Require customized assistance for a multifaceted solution

When an Adobe solution is at the heart of your business, the ability to maximize your investment depends on how effectively you can put the technology to work. The Extended Service customer care offering for Adobe Document Cloud eSign services helps you make the most out of your investment in e-signatures. Get a program tailored to your needs, with direct access to a designated technical solution manager who is familiar with your environment and business objectives.

The Extended Service customer care offering is a comprehensive set of proactive services, designed to eliminate any technical barriers to your business success. It has been created specifically to enhance and extend the services you already receive as an Adobe Document Cloud eSign services customer.

Service enhancements

The Extended Service offering is available only to Document Cloud eSign services customers as an annual subscription and requires an annual commitment.

	Service included with Document Cloud eSign services	Extended Service
	included	additional cost
How-to support	✓	✓
Enhanced service levels	✓	✓
Direct access to experts	✓	✓
Escalation management	✓	✓
24x7 support availability	✓	✓
Designated technical solution manager		✓
Priority case routing		✓
Proactive case monitoring		✓
New release enablement		✓
Customized technical engagement		✓
Incident history reviews		4/year

Service definitions

How-to support—You can receive answers to your critical questions about Adobe Document Cloud via web, email, live chat, telephone and the Adobe Document Cloud community.

Enhanced service levels—Get industry-leading, enterprise-class availability and response times, for both customer service and technical support issues.

"Adobe is a trusted business partner and our relationship with the company was key to our decision to adopt eSign services in Adobe Document Cloud. The ongoing support from Adobe has been exceptional, which helps us address our business needs today and into the future."

Joost van de Bunt, business development manager, KLM

Direct access to experts—Directly access a technical solution manager by phone, web or chat who can help with your questions. Consult our growing online Knowledgebase of technical solutions, documentation, FAQs, training videos and more anytime. Connect with other customers to share best practices and lessons learned.

Escalation management—Should your business need require escalation, a technical solution manager will manage it.

24x7 support availability—Support for critical issues anytime your business needs help.

Designated technical solution manager—A designated technical solution manager is assigned to be your primary point of contact for support.

Priority case routing—Cases will be directly routed to your designated technical solution manager, who will leverage the best Adobe resources on your behalf.

Proactive case monitoring—Your designated technical solution manager will actively monitor open cases and take proactive steps to promote the timely resolution of issues.

New release enablement—Learn about new release features and get advice on how best to take advantage of them in your environment.

Customized technical engagement—This service enhancement includes documentation tailored according to your particular situation and use case, remote participation to address the specific needs triggered by your business-critical events and verification of the technical health of your environment.*

Incident history reviews—Gain in-depth reviews of responsiveness, solutions provided, case history, satisfaction and future potential use cases.

Customer care response objectives

All Adobe Customer Care offerings provide high-touch expert coverage to achieve the highest level of responsiveness. For all customer care offerings, the response time and actions we take are based on an assessment of the impact of the reported technical issue on your business, as described below. The more serious the business impact, the higher the assigned priority.

Priority	Description	Response Time
P1	Mission Critical. Essential services are down, causing critical impact to business operations; no workaround is available.	30 minutes
P2	Urgent. Essential services are significantly degraded or impacting significant aspects of business operations.	2 hours
P3	Important. Services are noticeably impaired, but most business operations continue as normal.	4 hours
P4	Minor. The support request consists of "how to" questions, enhancement requests or documentation questions.	1 business day

For more information

To learn more about the Extended Service offering, contact your Adobe sales representative or customer success manager.

*Typically, engagement is a prescheduled, 30-minute session, with up to four sessions per year. Large-scope requests may require professional services at an additional cost.



Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2015 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

Deliver dynamic digital services with Adobe Sign

Speed signature processes and deliver cost-effective digital services with trusted, legal electronic signatures



Adobe Sign includes:

- Cloud-based e-signatures
- Web and mobile apps
- Administration and workflow control
- Flexible APIs and turnkey integrations

State and local governments are continually looking for service improvements and efficiencies. Yet processes that require signatures continue to delay government business—consuming unnecessary resources and introducing compliance risk. Electronic signatures (e-signatures) have been legal and enforceable since the Electronic Signatures in Global and National Commerce Act (ESIGN Act) was passed in 2000. With today's tight budgetary and regulatory constraints, governmental agencies of all sizes are looking to e-signatures as a way to complete transactions faster and easier. Electronic signatures are becoming the preferred way for governments to transform the resource-intensive, manual process of securing signatures and approvals.

Automate signing and approvals across agencies and departments

Adobe Sign helps you digitize entire signing processes, from document creation, collaboration, and execution to archiving and management—speeding signature workflows and reducing costs. With Adobe Sign, you can reduce signing and approval processes from days to minutes, improve efficiency and mobility, and help ensure security and compliance for your most critical data. State and local governments choose Adobe Sign to automate signing processes because of its intuitive user experience, robust capabilities, strong security, and ability to be configured to comply with specific legal requirements, as well as its flexible APIs and turnkey integrations.

Adobe Sign can speed every agency and department's processes, such as:

- Licensing
- Service registration
- Approvals and authorizations
- Benefits enrollment and administration
- Inspections
- Permitting
- Court orders
- Supplier agreements
- RFPs and contracts
- Hiring and onboarding
- Applications and forms
- Payroll

Create exceptional experiences for everyone

With Adobe Sign, you can send digital documents for signature with a single click, and signers can e-sign documents from anywhere using a web browser or mobile device. Documents are guarded with strict security, and can be accessed, tracked, and managed from anywhere in real time.

With Adobe Sign, you can:

- **Prepare documents for signature**—Whether existing or new, quickly prepare documents for signature. Add signature and form fields, and use intuitive tools to assist with layout.
- **Request signatures from others**—Send to one or more recipients, in any order. With a few quick clicks, they can review and e-sign—anytime, anywhere, on any device.
- **Track and manage**—Track document status in real-time. Get notified when people sign. Send reminders and maintain an audit trail automatically.
- **Send one document to many people**—Each recipient gets a personalized version to sign.
- **Work from favorite applications and devices**—Work conveniently from web or mobile, or work from other applications—including Adobe Acrobat DC, Microsoft Word, and Microsoft PowerPoint.

"Driven by overall consumer and enterprise digitization trends, e-signatures are on the rise."

Craig Le Clair, Forrester Research, Inc.
Brief: E-Signature Transactions Topped
210 Million in 2014, May 2015

"The same customer expectations in the commercial world are redefining constituent expectations in the public sector..."

Andrew Bartels and Chip Gliedman,
Forrester Research, Inc.
US Government Spending and
The BT Agenda, March 2015

For more information

<https://adobe.com/go/adobesign>



Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe Sign automates e-signature processes, including:

- **Extending existing business systems with e-signatures:**

- Use our flexible APIs to incorporate e-signatures into your enterprise systems and applications.
- Easily add e-signatures using our turnkey integrations for leading applications, including Ariba, Workday, SAP, Apttus, and more.

- **Simplifying and speeding signature workflows**—Create easy-to-follow custom workflows with templates or deploy stand-alone, self-serve web applications for signature-based business processes.

- **Embedding signable forms into a web page**—Post signable documents or forms on a website so that constituents can sign agreements easily—and you can route for countersignatures, if needed.

- **Branding the signing experience**—Easily specify your agency or department logo, tagline, and key messages to customize the signing experience for your constituents.

- **Enhancing security with two-factor authentication**—Add an extra level of verification to signature workflows. Request a password, use phone authentication, require login with a social identity, or use Knowledge-Based Authentication (KBA).*

- **Using advanced digital signatures**—Deploy flexible workflows to meet advanced signing requirements and industry-specific regulations with certificate-based digital signatures.

Work with the digital document leader

From the global leader in secure digital document solutions for more than 20 years, Adobe Sign is trusted and used by many federal, state, and local agencies, as well as Fortune 1000 companies worldwide. By removing the friction and delays created by paper-based signatures, Adobe helps government agencies and departments of all sizes streamline services —providing their staff and citizens with efficiency gains and better signing experiences while reducing the costs and resources involved with signature processes.

Use Adobe Sign to:

- **Accelerate critical signing processes by 500% or more**—Adobe Sign saves time and money by reducing or eliminating manual or paper-based processes—plus the cost, errors, and delays that go with them. Real-time tracking and management increases process transparency, improves turnaround times, and frees your employees to focus on more important tasks.
- **Create exceptional signing experiences**—Adobe solutions transform state and local government services with fast response times and speedy signing processes. Sign from anywhere without printing or faxing documents, installing software, creating new logins, or scanning anything. Entire signing processes can be completed in just minutes from start to finish.
- **Meet demand for mobile solutions**—Workers can connect and stay productive wherever they go. Using a smartphone or tablet, they can access stored documents, collect signatures in person, send documents for signature electronically, and manage the signing process quickly and easily.
- **Protect sensitive information and transactions**—Backed by hundreds of security features, processes, and controls, Adobe Sign is certified compliant with rigorous security standards, including SOC 2 Type 2, ISO 27001, and PCI DSS used in the Payment Card Industry. Adobe Sign can also be configured to support compliance with industry-specific regulatory requirements, such as HIPAA, FERPA, GLBA, and FDA 21 CFR Part 11.

To learn more about how Adobe Sign can benefit your agency or department, contact your Adobe sales representative today.

* KBA available in the United States only

Adobe, the Adobe logo, and Acrobat are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2016 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

Training and Other Materials, Samples, or Examples

Attachment O- Admin Guide (pg 289)

Attachment X- Implementing Adobe Sign (pg 354)

Attachment Y-Adobe Sign User Guide (pg 374)

Adobe Sign

Admin Guide

Table of Contents

Welcome to Adobe Sign!	4
Account Setup	5
External Archive	5
How to set it up	5
Branding your account	6
Company name and URL hostname	6
Upload your logo	8
Add an email header and footer	9
SecuritySettings	15
User Access Security - SAML	15
User Access Security	16
Transaction Security	18
Post-Transaction Security	20
Account Sharing	22
Advanced Account Sharing (Enterprise only)	22
AgreementSettings	23
Recipients	23
Recipient Roles	23
Recipient Groups	24
Recipient Authentication	24
Setting message templates (Business and Enterprise)	26
Message Templates	27
How users can attach or choose documents	27
Attaching Documents	28
Setting default reminders	29
Reminders	29
Setting a default document expiration	29
Document Expiration	30
Users andGroups	31
Users	31
User page features	31
How to Create a User	32
How to Deactivate/Reactivate a user	34
How to promote a user to admin	37
Creating Users in Bulk	39
Groups (Business and Enterprise)	42
How to Create a Group	42
How to Add Users to a Group	43

Moving a single User via the User profile	43
Moving multiple Users using Bulk User Edit.....	44
Assign Users to Group from within the Group Settings.....	46
Group level Admin authority controls.....	49
Adjusting Group level settings.....	50
Library Templates	52
Creating a Reusable Document	53
Editing Template Permissions.....	56
Reports (Adobe Sign – Business and Enterprise)	58
Report Parameters	60
Report Results	63

Welcome to Adobe Sign!

Before you begin using your Adobe Sign account, we've got some suggested steps to getting your account setup and customized for your company's use. The purpose of this guide is to get you up and running with branding, security settings, users and templates.

This guide is outlined in such a way that as you move through the "chapters", you'll cover all the important features and settings. By the end, your account will be up and ready to go. Keep in mind, there are plenty of other options and settings to explore that aren't covered in this guide. Our knowledge base is an excellent resource for getting information on the other settings that can be found in Adobe Sign.

Now sit back, login and let's get you e-Signing!

Account Setup

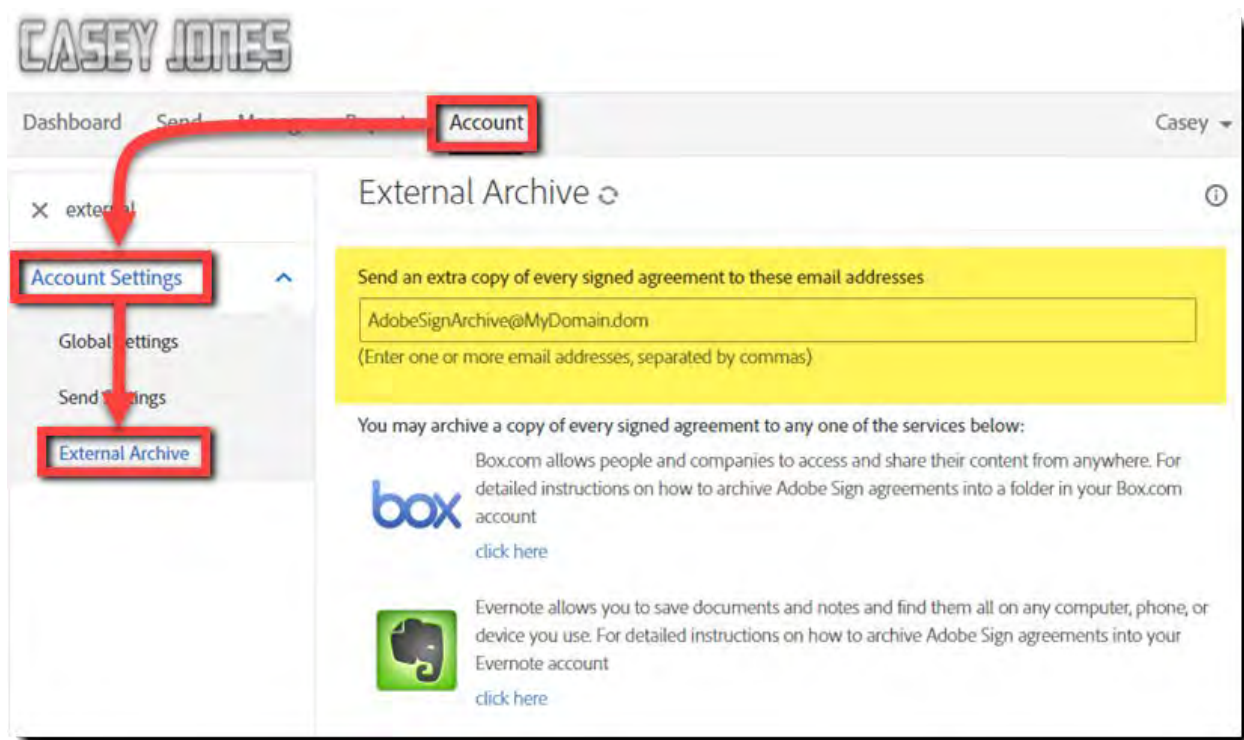
This section will go over the suggested steps for initially setting up your account.

External Archive

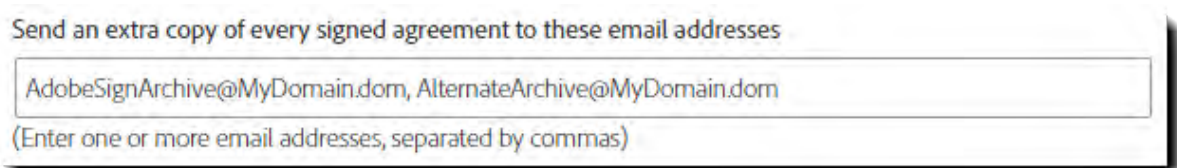
Like backing up your computer or phone, it's a good idea to keep copies of your signed agreements. Instead of downloading the agreements one by one from the Manage page, the External Archive can send a copy of signed agreements to an alternate email address, an Evernote account or a Box account.

How to set it up

Log in as an Account Admin, and navigate to: **Account > Account Settings > External Archive**




To have copies of your account's agreements send to an alternate email address, enter that email address into the **Send an extra copy...** field and click the **Save Changes** button.




To have a copy sent to either Evernote or Box, click the corresponding **click here** link and specific instructions will pop-up in a new window.

You may archive a copy of every signed agreement to any one of the services below:



Box.com allows people and companies to access and share their content from anywhere. For detailed instructions on how to archive Adobe Sign agreements into a folder in your Box.com account [click here](#)



Evernote allows you to save documents and notes and find them all on any computer, phone, or device you use. For detailed instructions on how to archive Adobe Sign agreements into your Evernote account [click here](#)

Branding your account

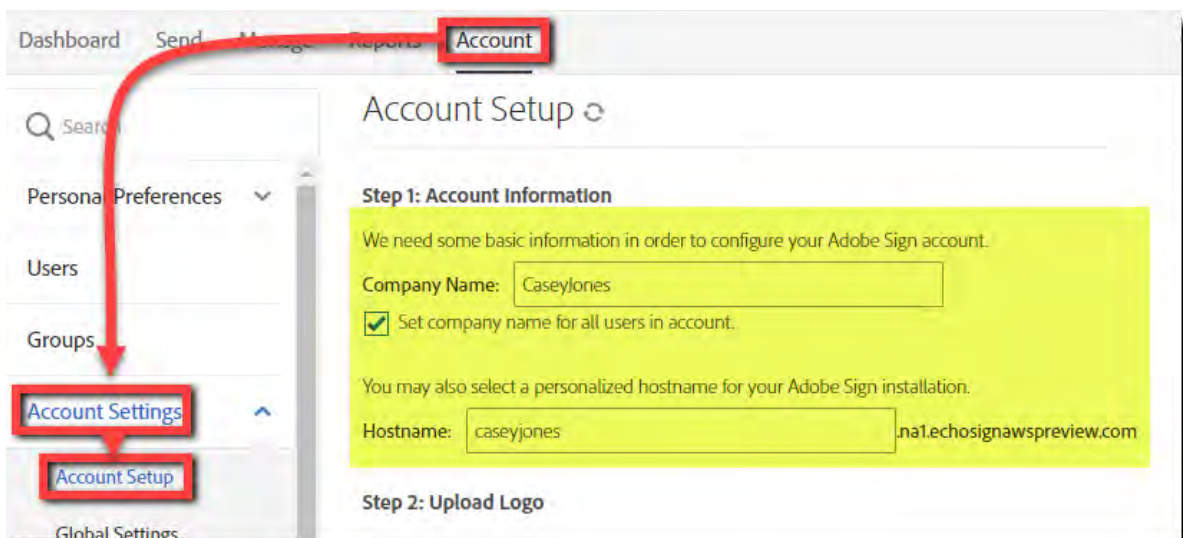
Adding your company branding is an excellent way to customize Adobe Sign for the users in your account, as well as your signers.

Company name and URL hostname

In this section, you will set the company name and a hostname for your account. These may seem basic, but they will personalize your account.

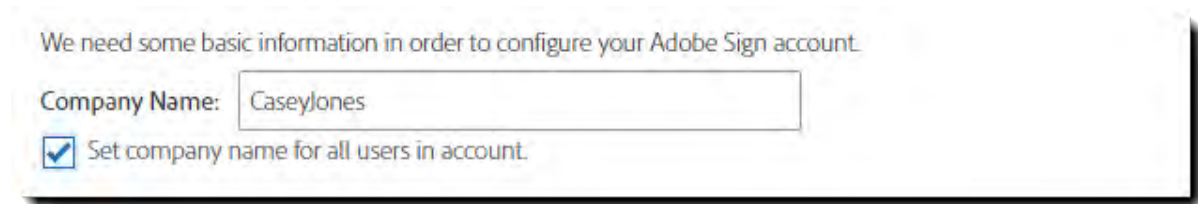
These two settings are Account wide and cannot be adjusted at the Group level

Log in as an Account Admin and navigate to: **Account > Account Settings > Account Setup**



Company Name

The value you enter into this field will be displayed in all email correspondence from Adobe Sign. This is also automatically populated into Company Name fields for your users when they need to sign a document.



We need some basic information in order to configure your Adobe Sign account.

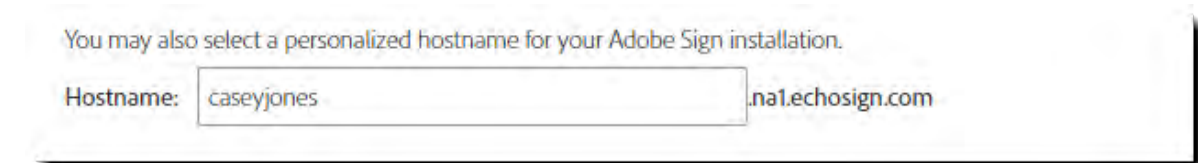
Company Name:

☒ Set company name for all users in account.

By default, Adobe Sign permits users to edit their personal settings, and this includes the Company Name value for their individual user. If you would prefer to install one immutable Company name to all users, you can check the **Set company name for all users in account** box.

Hostname

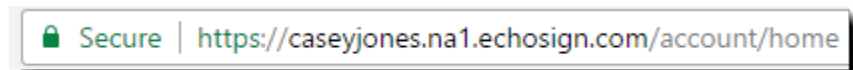
Setting the hostname for your account changes the URL your users log in to and the URL where agreements are hosted for your signers.




You may also select a personalized hostname for your Adobe Sign installation.

Hostname: .na1.echosign.com

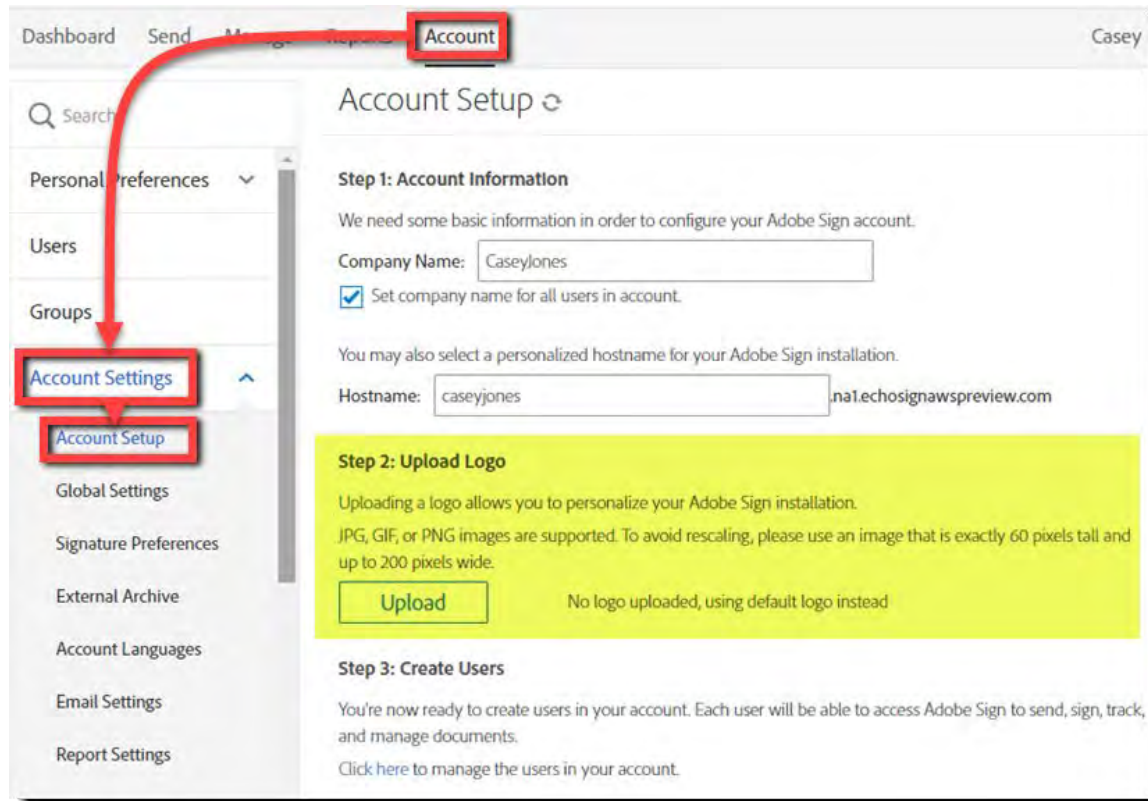
The result is a customized URL with your hostname.



 Secure | <https://caseyjones.na1.echosign.com/account/home>

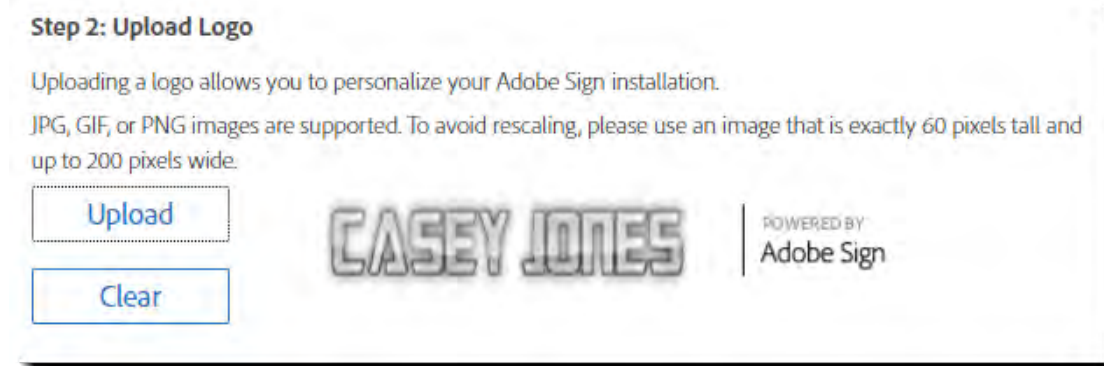
Upload your logo

Log in as an Account Admin and navigate to: **Account > Account Settings > Account Setup > Upload Logo**.



Click the **Upload** button and navigate to the image you want to use. Keep in mind, images of the stated dimensions (60 pixels tall and 200 pixels wide) work the best.

Once you've chosen an image, the logo will be displayed to the right of the *Upload* button:



If you need to change the logo at any time, click the **Clear** button and the logo will be removed.

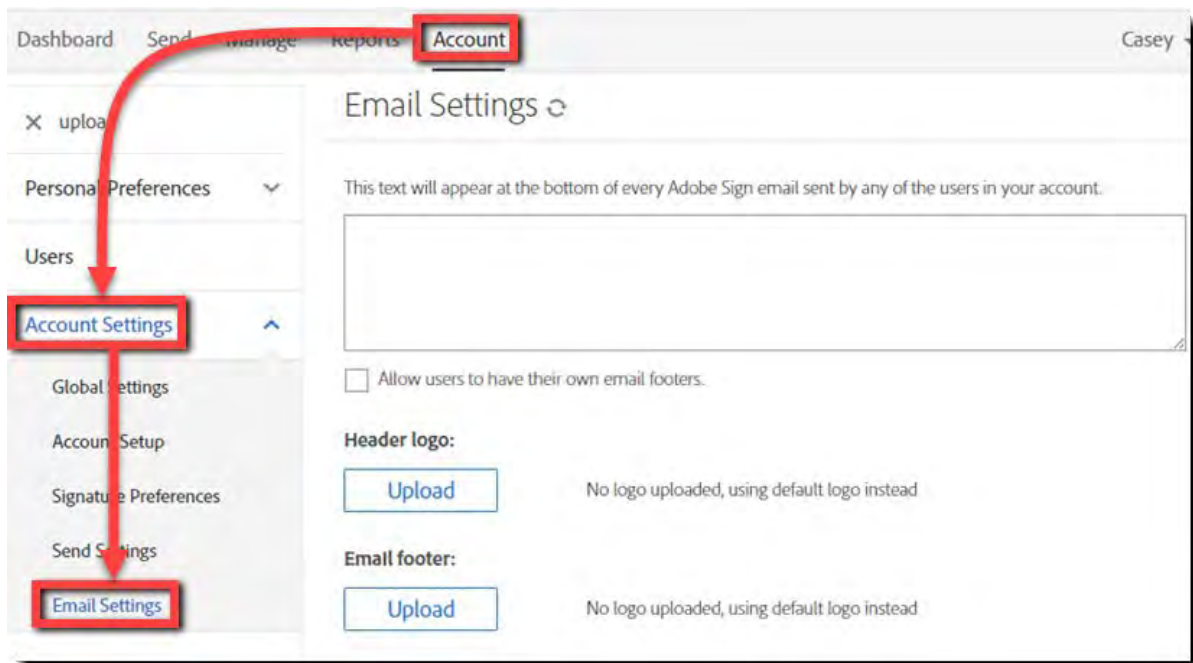
Add an email header and footer

Get your branding into your Agreement emails by setting a custom image for the header and/or footer of the email template.

Additionally, you can provide an optional Account wide plain text footer for marketing, legal information or any other content you want distributed with your Agreement notifications.

To add or edit your existing header/footers:

Navigate to: **Account > Email Settings** then **Header & Footer Images**



Plain Text Footer

At the top of the page is the plain text footer. This footer is Account wide, and cannot be overridden at the Group level.

Email Settings

This text will appear at the bottom of every Adobe Sign email sent by any of the users in your account.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget rhoncus est. Donec sit amet porttitor eros, at fermentum metus. Aliquam luctus eleifend est sed vulputate. Mauris in tortor eleifend, hendrerit tellus vel, luctus nulla. Suspendisse potenti. Proin blandit eu felis nec cursus. Integer vitae posuere nibh, nec sodales magna. Nam sodales elementum orci, a efficitur nisl consectetur eget. Morbi sed metus mauris. Sed nisl velit viverra vel luctus sit amet, pellentesque sed turpis. Praesent dignissim mi massa, varius sodales.

☐ Allow users to have their own email footers.

Header logo:

Upload


No logo uploaded, using default logo instead

Email footer:

Upload

No logo uploaded, using default logo instead

This text will be displayed below the page thumbnail and message content of the Agreement



globalcorp
CLIENT SERVICES AGREEMENT

Client Information	
Company Name	Example Corp
Address	1234 Main Street San Jose, CA 95131
Phone	
Email	
Order Number	123456789

Client Services	Amount
New Client onboarding	
Training and consultation	
Software licenses and support	
Implementation and integration	
Project management	
Project completion	\$1,200.00

GlobalCorp, Inc. ("GlobalCorp") is a company that provides software, services, and support to its clients. This Agreement, along with the terms and conditions of use, constitutes the entire agreement between you and GlobalCorp. Please read this Agreement carefully before you agree to it.

Step 1: Authorize the Service Agreement Details

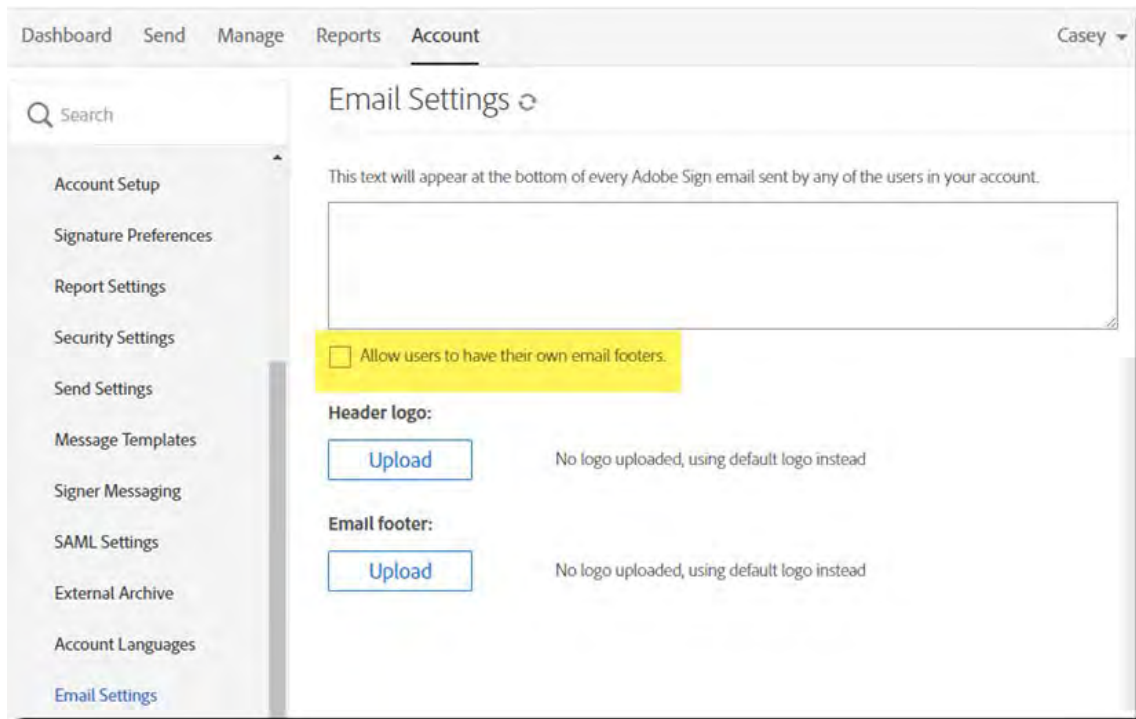
Casey Jones Has Sent You GlobalCorp Client Services Agreement to Sign

If you need to delegate this document to an authorized party for signature, please do not forward this email. Instead, [click here](#) to delegate.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget rhoncus est. Donec sit amet porttitor eros, at fermentum metus. Aliquam luctus eleifend est sed vulputate. Mauris in tortor eleifend, hendrerit tellus vel, luctus nulla. Suspendisse potenti. Proin blandit eu felis nec cursus. Integer vitae posuere nibh, nec sodales magna. Nam sodales elementum orci, a efficitur nisl consectetur eget. Morbi sed metus mauris. Sed nisl velit viverra vel luctus sit amet, pellentesque sed turpis. Praesent dignissim mi massa, varius sodales ligula interdum sit amet. Proin orci mauris, porttitor vulputate ultrices nec, consectetur non nulla. Quisque non interdum nunc. Suspendisse potenti. Praesent diam ligula, dignissim eu eros et, hendrerit dignissim lacus. Praesent efficitur rutrum tellus non venenatis.

User Level Footers (Signature Files)

By checking the **Allow users to have their own email footers** box, you allow each user to optionally include their own personalized footer, much like a signature file in email.

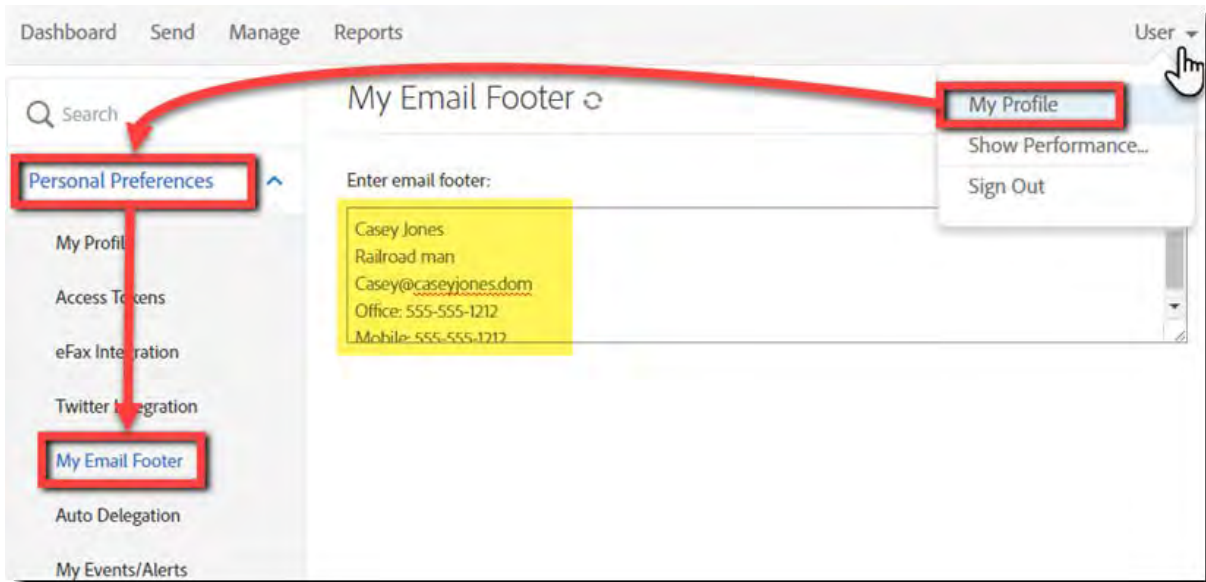


This footer is in **addition** to the Account wide footer, and any image footer that may be applied.


Users can set their individual footers by:

- Mouse over the user name in the upper-right corner of the screen to open the menu, and select **My Profile**
 - The page will refresh and display the User menu with *Personal Preferences* already expanded
- Select **My Email Footer** to open the page

Note: This option is only visible after the Account admin enables the setting



The user footer is inserted between the thumbnail image and the Account level text footer:



Casey Jones Has Sent You GlobalCorp Client Services Agreement to Sign

Casey Jones (CaseyJones) says:
"Please review and complete GlobalCorp Client Services Agreement."

[Click here to review and sign GlobalCorp Client Services Agreement.](#)

After you sign GlobalCorp Client Services Agreement, all parties will receive a final PDF copy by email.

If you need to delegate this document to an authorized party for signature, please do not forward this email. Instead, [click here](#) to delegate.

Casey Jones
 Railroad man
 Casey@caseyjones.dom
 Office: 555-555-1212
 Mobile: 555-555-1212

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Fusce eget rhoncus est. Donec sit amet porttitor eros, at fermentum metus. Aliquam luctus eleifend est sed vulputate. Mauris in tortor eleifend, hendrerit tellus vel, luctus nulla. Suspendisse potenti. Proin blandit eu felis nec cursus. Integer vitae posuere nibh, nec sodales magna.

To ensure that you continue receiving our emails, please add echosign@echosign.com to your address book or safe list.

Header and Footer Images

The default email header mirrors the header you see if you log into your Adobe Sign account. It will contain either the default Adobe Sign logo, or the logo you have uploaded for your account/group.

The email image header will always be at the very top of the email content.



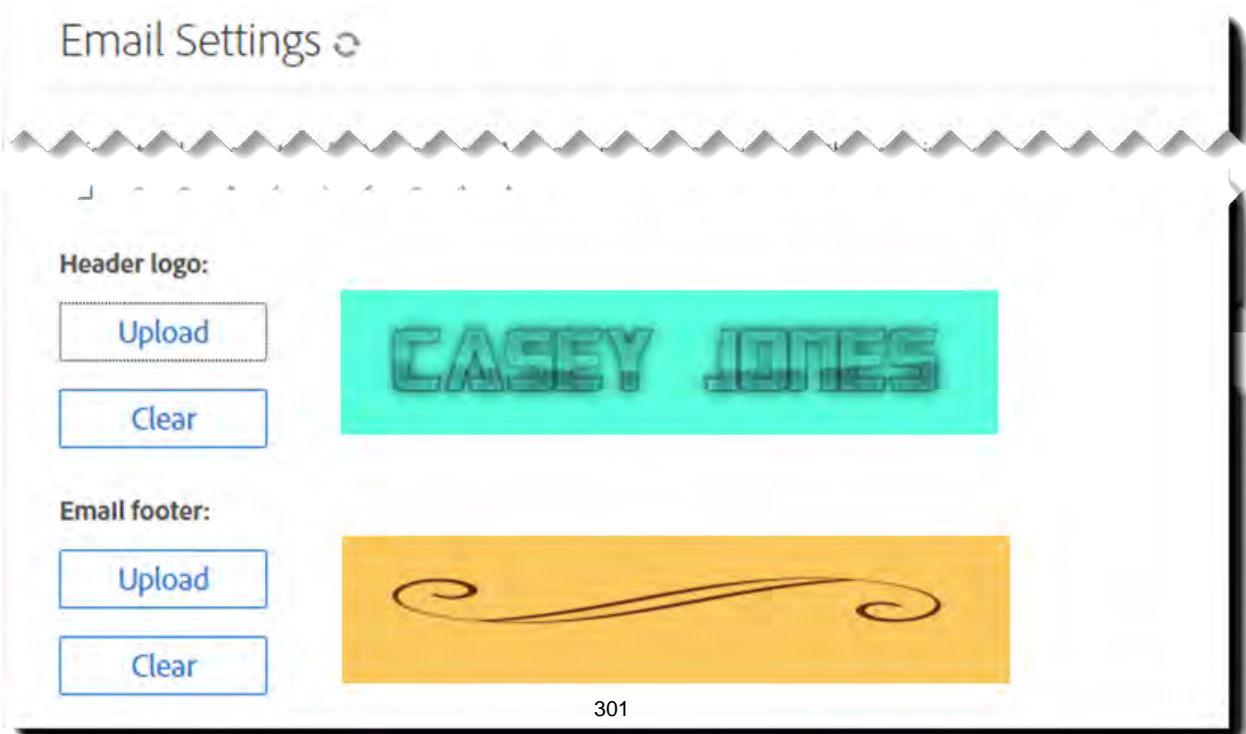
The default footer image is empty. If you insert a footer image, it will display at the bottom of the email (with only the safe listing message below it).

Both the email header and footer images need to be 600x200px graphics (png, jpg or gif).

To install either image:

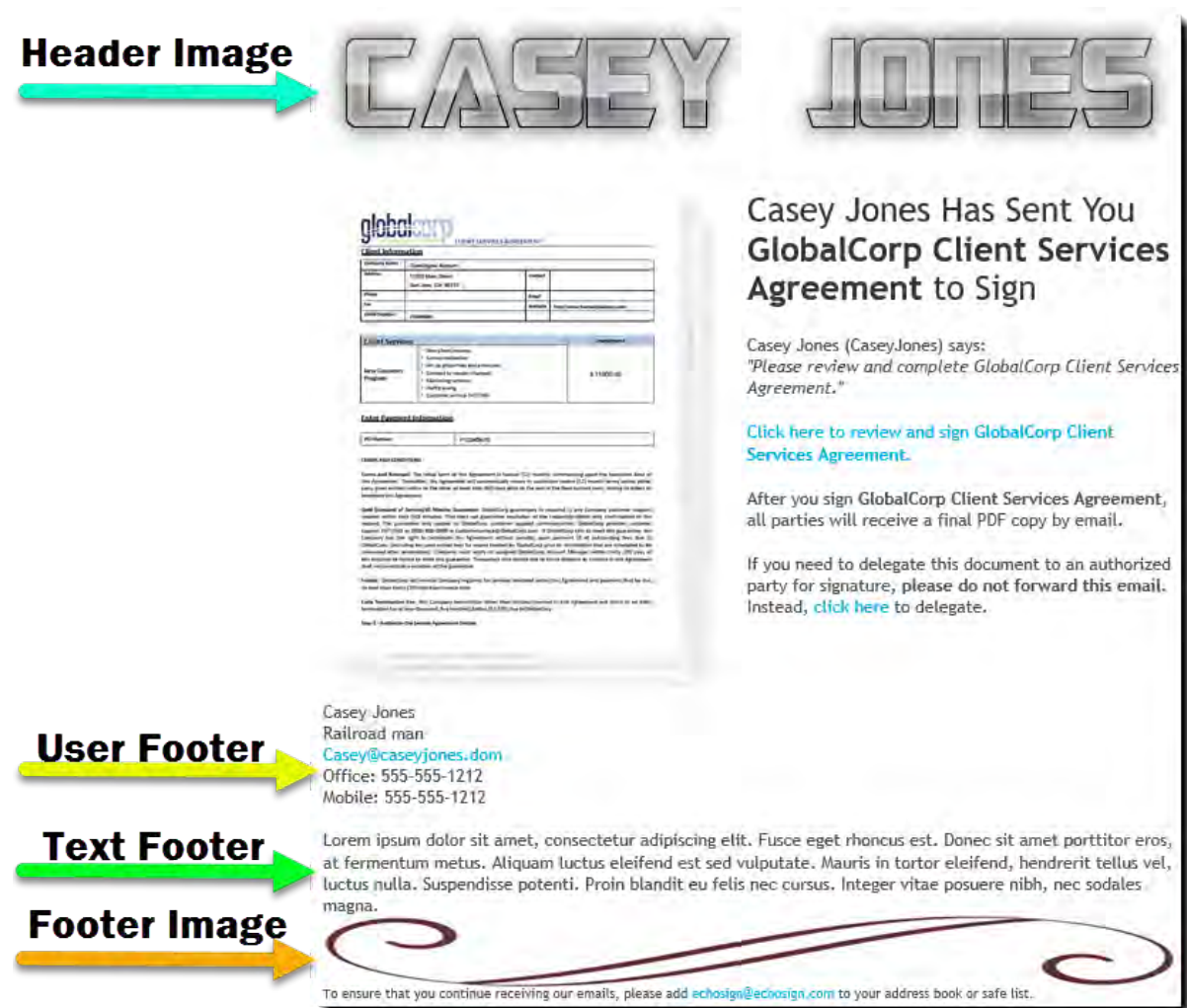
Click on **Upload** button, navigate to the image you want to upload and select it.

Once uploaded, the graphic will appear to the right of the button.



You can remove the image by clicking the **Clear** button at any time.

Below is an example of a fully branded email:



Email header and footer images can also be set at the Group level (which will override the Account image).

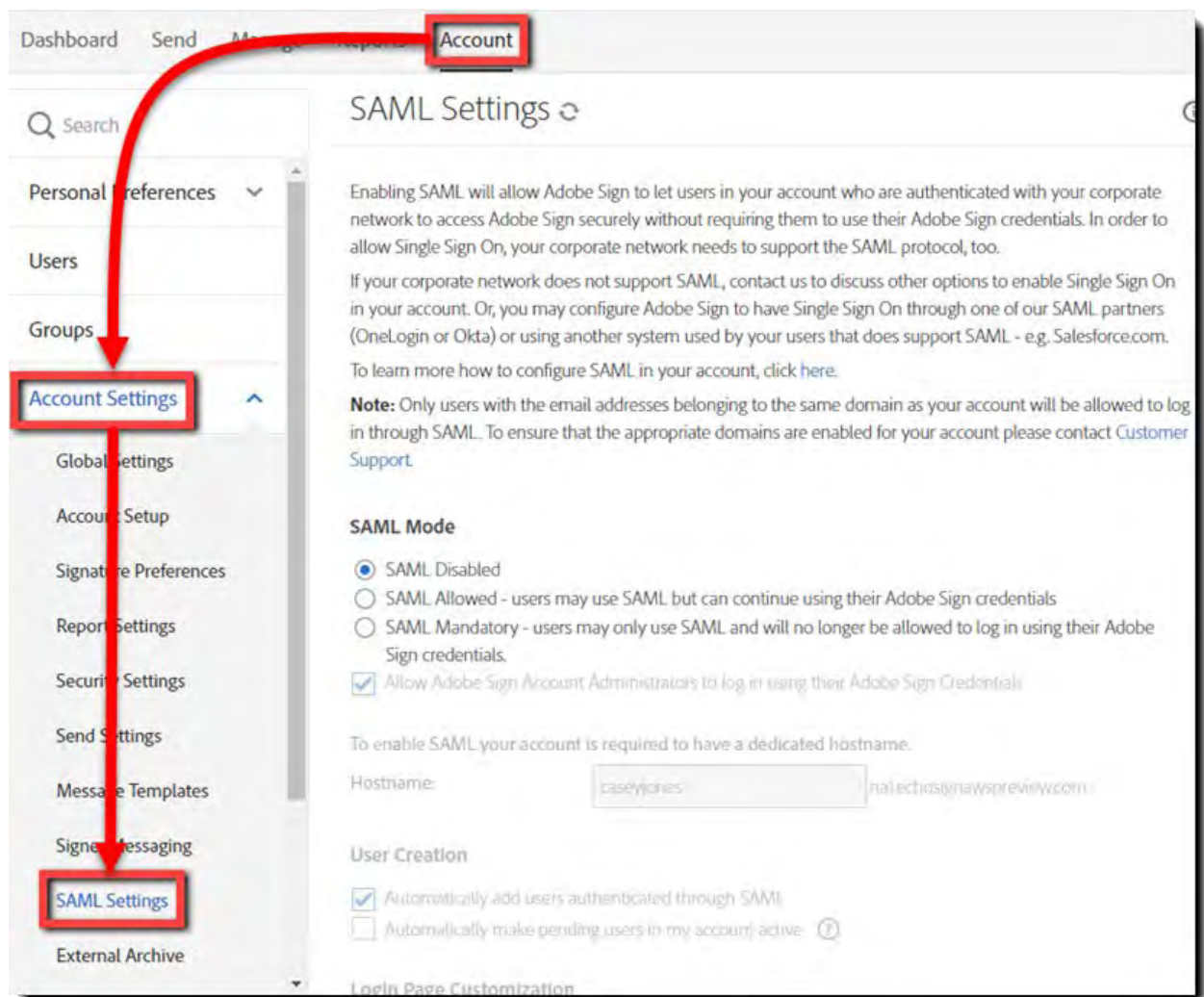
Security Settings

Account, user and document security is Adobe Sign's number one concern. Therefore, we provide several security options at the account level. We suggest reviewing the settings in this section and decide which will work the best for your use case.

User Access Security - SAML

If your company has a federated log in solution, Adobe Sign does provide [SAML 2 options](#) for user authentication. Configuring SAML will require that you [claim your domain names](#).

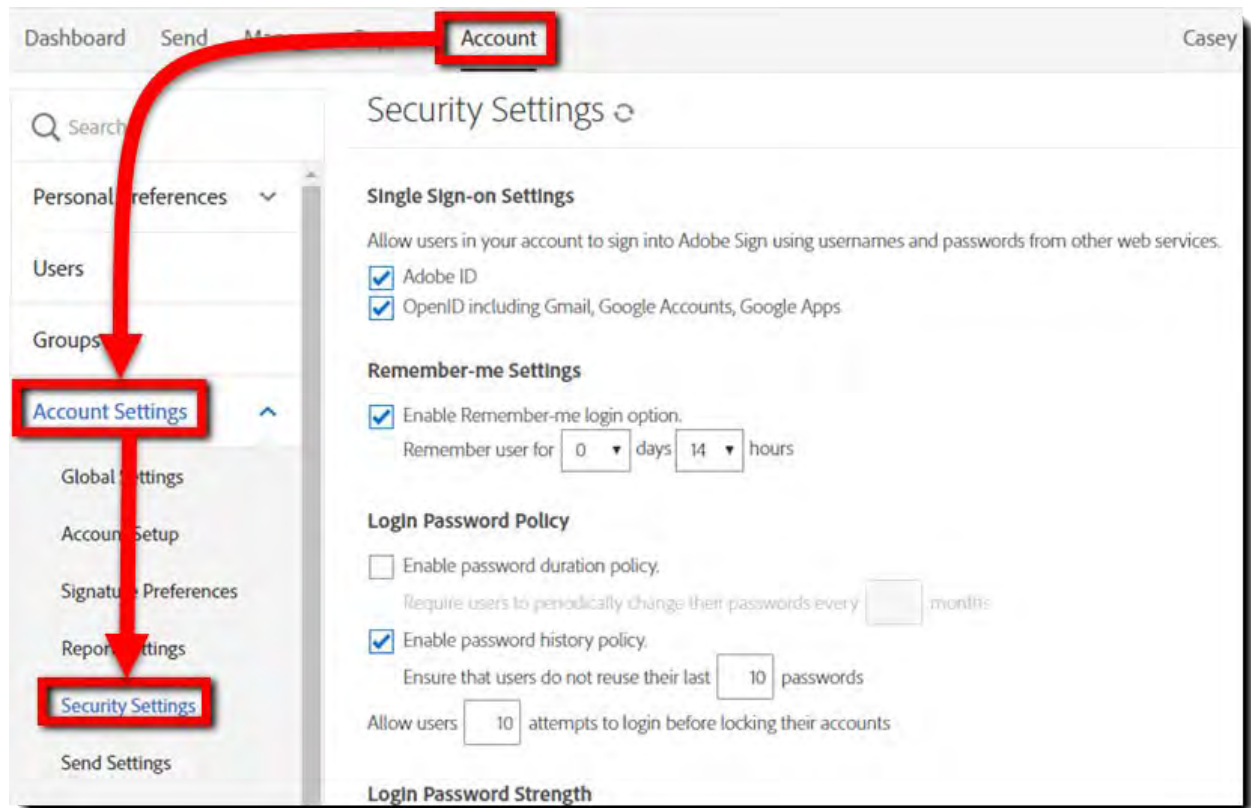
Adobe Sign SAML settings can be found by navigating to: **Account > Account Settings > SAML Settings**



User Access Security

Authentication to the Adobe Sign app has multiple settings available so you can configure the security criteria to match your company policy regarding access.

User access security settings can be configured by navigating to: **Account > Account Settings > Security Settings**



Single Sign-on Settings

You can either allow or deny users in your account the ability to log in to Adobe Sign by authenticating through other services. It is recommended that you disable either (or both) of these settings if they are not used to keep the log in process to a single simple option for users.

Single Sign-on Settings

Allow users in your account to sign into Adobe Sign using usernames and passwords from other web services.

- ☒ Adobe ID
- ☒ OpenID including Gmail, Google Accounts, Google Apps

Remember-me Settings

Enable this setting to enable the *Remember Me* setting when authentication to Adobe Sign. This setting remembers the authentication to the service (on the local system) for the time frame selected.

Remember-me Settings

☒ Enable Remember-me login option.
Remember user for days hours

Login Password Policy

The options under **Login Password Policy** set whether users should be required to change their password after a number of months, whether a previous password can be used as their new password, and how many log in attempts can be made before their userID is locked.

Login Password Policy

☒ Enable password duration policy.
Require users to periodically change their passwords every months

☒ Enable password history policy.
Ensure that users do not reuse their last passwords

Allow users attempts to login before locking their accounts

Login Password Strength

This setting allows you to adjust the strength or difficulty of the password set by users in your account.

Login Password Strength

- ☐ Standard - At least 8 characters, must include lower case, upper case, number and symbol
- ☒ Medium - At least 10 characters, must include lower case, upper case, number and symbol
- ☐ Strong - At least 12 characters, must include lower case, upper case, number and symbol

Allowed IP Ranges

This option will only allow authentication to the Adobe Sign application when the request is coming from the specified IP address ranges.

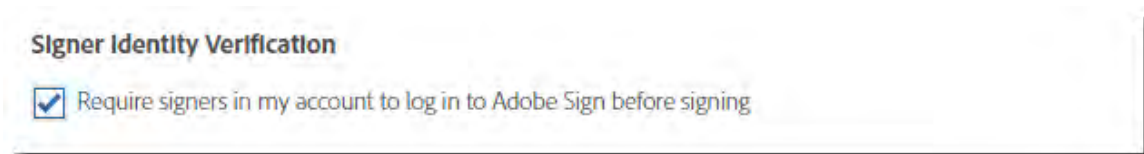


The screenshot shows the 'Allowed IP Ranges' settings panel. At the top, there is a checked checkbox with the text 'Only allow access to the system from IP addresses that are listed below'. Below this is a search bar with a magnifying glass icon and the word 'Search'. To the right of the search bar are a plus icon and a hamburger menu icon. Below the search bar is a table with a header 'IP/Range' and a single entry '192.168.0.1/8'.

IP/Range
192.168.0.1/8

Signer Identity Verification

If your users will be signing documents, this option will require them to log in to Adobe Sign before they can apply their signature. This ensures the individual signing is either the user or someone with the user's credentials.



The screenshot shows the 'Signer Identity Verification' settings panel. It contains a checked checkbox with the text 'Require signers in my account to log in to Adobe Sign before signing'.

Transaction Security

This section pertains to the security controls that are in effect while an Agreement is going through the signature process. These settings can be found by navigating to: **Account > Account Settings > Security Settings**

PDF Encryption Type

This setting defines the type of encryption applied to the document once it has been sent through Adobe Sign. This encryption ensures the document can be opened but cannot be edited. Each version of the encryption is compatible with different versions of Acrobat. The recommended option is **128-bit AES** to ensure the document can be opened on most systems.

PDF Encryption Type

- ☐ 128-bit RC4 - Compatible with Acrobat 5.0 and later.
- ☒ 128-bit AES - Compatible with Acrobat 7.0 and later.
- ☐ 256-bit AES - Compatible with Acrobat X and later.

Agreement Signing Password

This setting applies to the Password Authentication option for recipients to access the document during the signature cycle. (Configured on the Send page when initially sending the agreement)

The setting limits how many attempts the recipient has to enter the correct password. Once this limit is exceeded, the Agreement is irrevocably **canceled**.

Agreement Signing Password

Apply a password policy when protecting document signing or viewing

☒ Restrict number of attempts.

Allow signer attempts to enter the agreement password before cancelling the agreement.

Agreement Signing Password Strength

This setting also applies to the Password Authentication option for recipients.

The feature allows you to adjust the strength or difficulty of the password your Senders need to enter.

Note: The password this setting governs is embedded in the PDF, and not stored in the Adobe Sign system. If it is lost, there is no option to recover it.

Agreement Signing Password Strength

- ☐ None - Any password is allowed
- ☐ Standard - At least 6 characters
- ☒ Medium - At least 7 characters, must include upper case or number
- ☐ Strong - At least 8 characters, must include lower case, upper case, and numbers

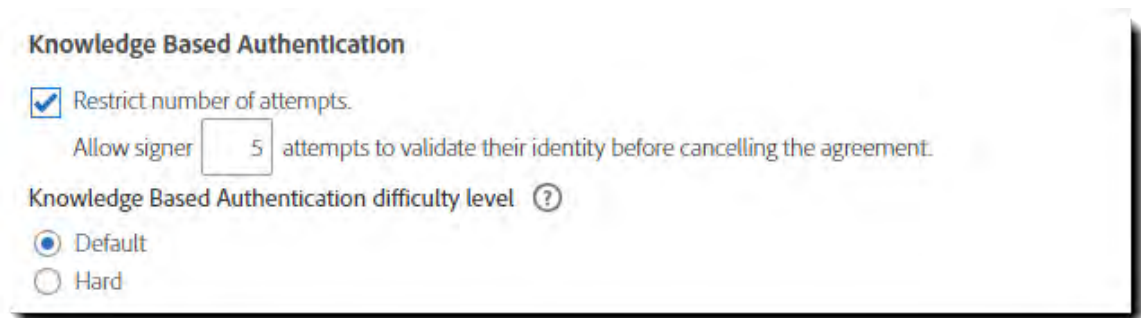
Knowledge Based Authentication

This option controls the Knowledge Based Authentication (KBA) option for recipients on the Send page.

This limit dictates how many attempts the signer has to pass the KBA in order to access the document. Once the limit is exceeded the agreement is canceled. The difficulty of the KBA is also set here.

- **Default** - Signers will be presented with 3 questions and will be required to answer them all correctly. If they only answer 2 correctly, they will be presented with 2 more questions and will be required to answer them both correctly.
- **Hard** - Signers will be presented with 4 questions and will be required to answer them all correctly. If they only answer 3 correctly, they will be presented with 2 more questions and will be required to answer them both correctly.

KBA requires a social security number, so is only viable for recipients in the US.



The screenshot shows the 'Knowledge Based Authentication' settings. It includes a checked checkbox for 'Restrict number of attempts.' Below this, a text input field is set to '5', followed by the text 'attempts to validate their identity before cancelling the agreement.' There is also a section for 'Knowledge Based Authentication difficulty level' with a help icon. Two radio buttons are present: 'Default' (which is selected) and 'Hard'.

Post-Transaction Security

These settings govern the PDF security of Agreements that have completed the signature cycle, and are fully executed.

Certify copy of the documents for

Find this setting by navigating to: **Account > Account Settings > Global Settings**

Adobe Sign will apply a Certificate (CDS) to any downloaded PDF for a completed transaction based on this setting. Certified PDFs readily show that the document has not been tampered with since being downloaded.

CDS will prevent any attempt to manipulate the PDF after download.

It is recommended that you enforce CDS at least for **external** recipients.

Certify copy of the documents for ?

- ☐ All recipients
- ☐ Internal recipients
- ☒ External recipients
- ☐ No one

Signed Document Password Protection

Find this setting by navigating to: **Account > Account Settings > Send Settings**

This setting allows, forces or denies Senders the ability to set a password for the **signed** document. (This is different from the optional password to access an Agreement *during* the signing process)

If allowed or enforced, the Sender needs to supply the password, and communicate that password to any party that needs to review signed documents.

Signed Document Password Protection ?

- ☒ Allow senders to password protect signed documents
- ☐ Enforce senders to password protect signed documents
- ☐ Do not allow

Note: This password is embedded in the PDF, and not visible anywhere in the Adobe Sign system. If you choose to use a password to lock access to the signed document, ensure you have a method in place to understand what those passwords are and retrieve them as needed.

Account Sharing

You can enable or disable the option for a userID to share the content of their user account to another userID.

Account Sharing

Find this setting by navigating to: **Account > Account Settings > Security Settings**

Account sharing allows one user to view (only) all the Agreement content of another user. This is great for managers that need to review the progress of their direct reports.

All shares that are created are one direction, there is no assumed reverse direction share that takes place.

If Account Sharing is enabled, the recommended option is to allow a user to ask to view another user's account.

Account Sharing

- ☐ Do not allow account sharing
- ☒ A user asking to view another user's account
- ☐ A user asking to allow another user to view their account
- ☐ Both

Advanced Account Sharing (Enterprise only)

For Enterprise customers that need to have a more “hands on” type of sharing that allows direct manipulation of agreements and library templates, Technical Support can enable Advanced Sharing.

Advanced Sharing is a one-way door. Once it is enabled, it changes the relationships of the shared objects in a way that cannot be reversed. For this reason, if you feel Advanced Sharing is important to your organization, it is recommended that you contact your Success Manager and have a trial account set up for you to test the functionality and verify it permits everything that you want to accomplish.

Agreement Settings

The settings in this section define the options available to a Sender when configuring an Agreement, and what the default value for those options will be.

In general, the recommendation is to reduce the number of options for the Sender to choose from or configure. Where possible, set a strong default value, and remove the option to edit that value.

This chapter will be broken into sections related to their effect on a transaction.

These settings can be found by navigating to: **Account > Account Settings > Send Settings**.

Note: These settings can be configured at the Group level to assure that each business unit can customize their sending experience and defaults as needed.

Recipients

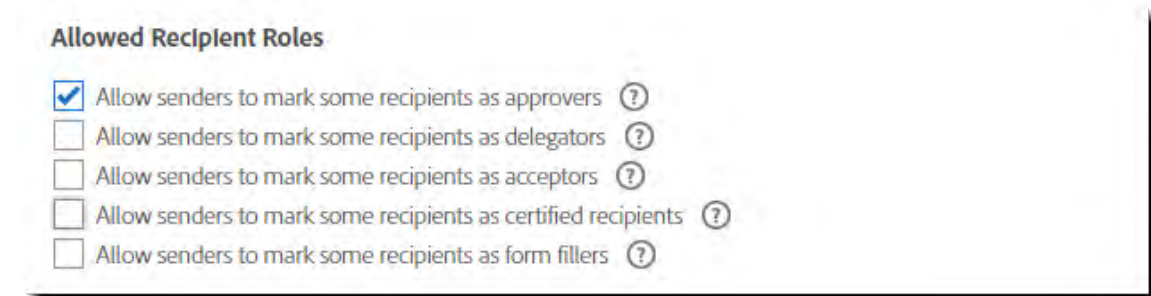
"Recipients" is a generic term that refers to any userID included in the signature cycle, regardless to the assigned role. The following settings will define what types of roles those recipients can have, and what level of identity authentication you want to employ

Recipient Roles

Depending on the level of service you have, you will have access to various "roles" that define what type of actions your recipients can perform in the Agreement. More details on the various role authorities can be found in the [knowledge base](#).

Allowed Recipient Roles

It is recommended that you only enable the roles you know you will need to better streamline the Senders experience.



Recipient Groups

Recipient Groups function as one signer, but that signer is a group of identified individuals. All members are notified at one time, and once one of the group members applies their signature, the Agreement moves to the next signer.

Recipient Groups

Enable this option if you have a need to define a group of signers for one signing event.



Recipient Authentication

Various methods of signer verification can be enabled for your users, with this setting. These methods are configured on the Send page as an element of the recipient record.

Identity Authentication Methods

It is recommended that you only enable the verification methods(s) that your internal policy demands.

- **Signing password** – Requires the signer to enter a predetermined password to sign the document. The password must be passed to the signer separate from the transaction. If this password is lost or forgotten, it cannot be recovered.
- **Knowledge based authentication** – Requires the signer to enter their Social Security Number and random identity questions will be generated by a third-party provider.
- **Social identity** – Requires signer to authenticate with one of the following services: Facebook, LinkedIn, Google, Twitter, Yahoo!, or Windows Live ID.
- **Phone (SMS)** - Requires the sender to provide a phone number for the recipient. The recipient will then get an 8-digit code they will enter and authenticate.

Identity Authentication Methods

Enable the following identity authentication methods for recipients

- ☐ Signing password [?](#)
- ☐ Knowledge based authentication [?](#) [Track Usage](#)
- ☐ Social identity [?](#)
- ☐ Phone authentication [?](#) [Track Usage](#)

By default, use the following method:

Email ▼

Sender settings

- ☐ Allow senders to change the default authentication method

Note: KBA and Phone authentication are metered authentication methods that incur an additional cost. It is advised that you only enable the authentication method(s) you have high confidence you will use.

By default, use the following method

This setting will define the default external recipient authentication method. Only options that have been enabled will be selectable in the drop-down list.

Sender settings

This option either allows or denies the Sender's ability to change the default authentication method defined. Enable this option only if there are known situations where the Sender has need to elevate the verification process from the default.

Internal Recipient Identity Authentication

Checking this setting allows Senders to set a different method of verification for recipients that are internal to your Adobe Sign account.

The general recommendation is to leave the internal signatures as email verification, providing less authentication friction to your employees that may need to counter-sign a large number of Agreements per day. By also enabling the [Signer Identity Verification](#) feature (Security Settings), you can passively gain password verification without the signer having to explicitly authenticate multiple times.

Identity Authentication for Internal Recipients

☒ Enable different identity authentication methods for internal recipients

Enable the following identity authentication methods for recipients

- ☐ Signing password
- ☐ Knowledge based authentication
- ☐ Social identity
- ☐ Phone authentication

By default, use the following method:

Email

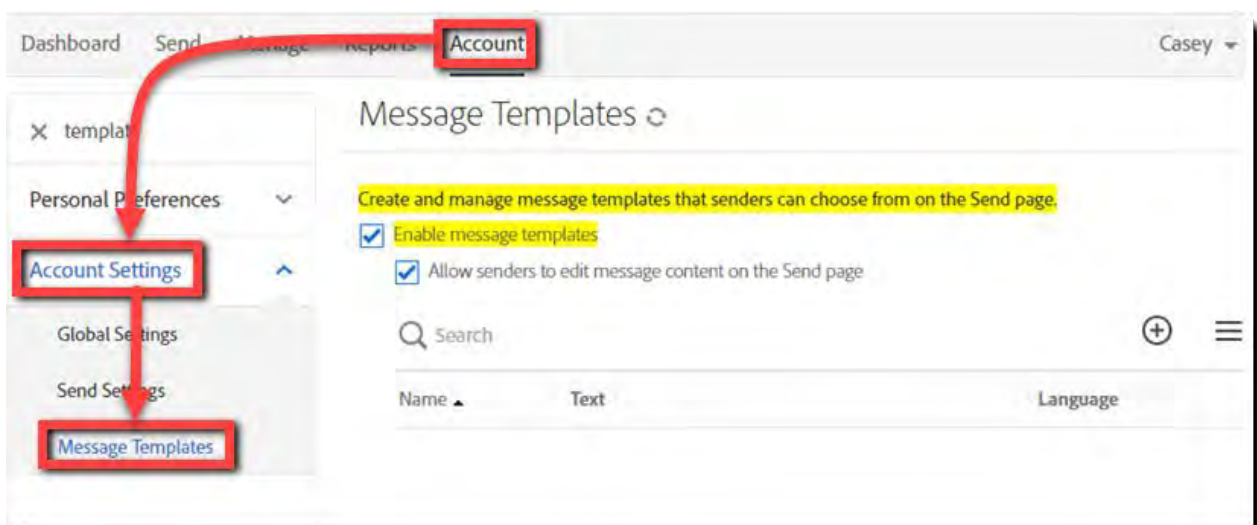
Sender settings

☐ Allow senders to change the default authentication method

Setting message templates (Business and Enterprise)

Enabling Message Templates for your account, allows the user to choose one of the email messages, predefined by you. This can ensure the correct message and information gets to your signers.

To enable message templates, navigate to **Account > Account Settings > Message Templates**

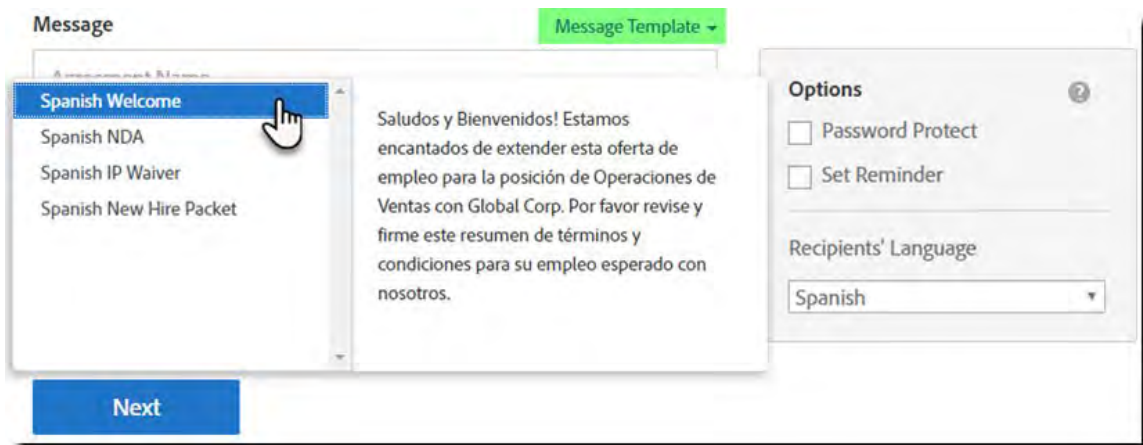


Message Templates

Enable message templates

Check the option to **Enable message templates**.

A link will be inserted at the top right of the message field (on the Send page) to allow selection of the template:



Note: For Enterprise customers, templates are linked to the *Recipients Language* option on the Send page. This limits the number of templates to scroll through for multi-language business units, and ensures that a message in the correct language is included.

Allow senders to edit message content

Either allow or deny users the ability to change the message template delivered to the Send page message field.

Enable this if you permit customizing Message content situationally.

How users can attach or choose documents

There is a lot of variability in how customers attach files to their agreements, and that is rooted in how the documents are created, managed and version controlled.

Customers that have “ad-hoc” files, content customized for each transaction, will likely need the ability to upload files from their local system. However, boilerplate templates that rarely change should ideally be served from one controlled source.

Attaching Documents

Attaching Documents

Please choose at least one way to attach documents

- ☐ Allow senders to attach documents from their computers
- ☒ Allow senders to attach documents from their document library
 - ☐ Include documents from the Adobe Sign shared library
- ☐ Allow senders to attach documents from Google Drive
- ☐ Allow senders to attach documents from Dropbox
- ☐ Allow senders to attach documents from Box.com

Allow senders to attach documents from their computers

Unchecking this option removes the **My Computer** link from the **Select Files** pop-up on the Send page.

Allow senders to attach documents from their document library

Unchecking this option removes the **Library Documents** link from the **Select Files** pop-up.

Include documents from the Adobe Sign shared library

Unchecking this option removes the I-9, W-4 and W-9 documents provided by Adobe Sign.

Allow senders to attach documents from Google Drive

Unchecking this option removes the **Google Drive** link from the **Select Files** pop-up.

Allow senders to attach documents from Dropbox

Unchecking this option removes the **Dropbox** link from the **Select Files** pop-up.

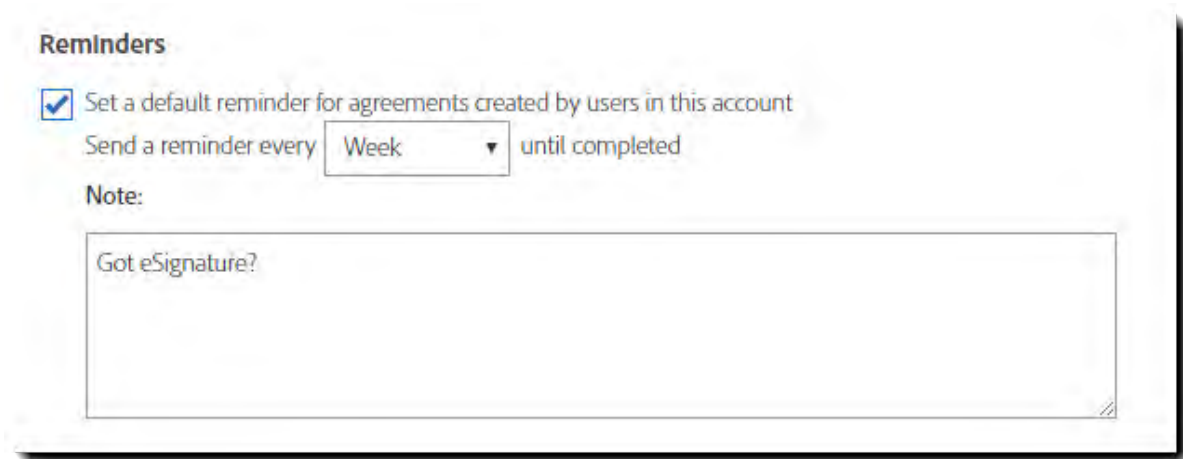
Allow senders to attach documents from Box.com

Unchecking this option removes the **Box.com** link from the **Select Files** pop-up.

Setting default reminders

Reminders are emails sent to the recipients of documents when it is their turn to act. On a Daily or Weekly cycle, a reminder email is sent to the recipient, letting them know the agreement is still waiting for them.

Reminders



The screenshot shows the 'Reminders' configuration section. It includes a checkbox labeled 'Set a default reminder for agreements created by users in this account' which is checked. Below this is a label 'Send a reminder every' followed by a dropdown menu set to 'Week' and the text 'until completed'. A 'Note:' label is positioned above a large text input field containing the placeholder text 'Got eSignature?'.

Set a default reminder for agreements created by users in this account

- Check the option to set a default reminder
- Choose the frequency in which you would like the reminder email sent
- The note entered will show in the reminder email sent to each recipient in turn

Note: Enabling default reminders will remove the option on the Send page for Senders to configure their own reminder, but still permits reminders to be configured on the Manage page.

Setting a default document expiration

In certain cases, you may want to expire or cancel documents that aren't signed after a certain number of days.

Once an agreement has expired, it cannot be restarted or retrieved and will show up under the Canceled/Declined section of the Manage page.

Document Expiration

Document Expiration

- ☒ Enable document expiration
 - ☐ Allow senders to set or modify expiration settings per document
 - ☒ Allow modification of expiration settings after document is sent
 - ☒ Limit number of days signers will have to sign documents to:
 - ☐ Include internal signers when applying document expiration deadlines
 - ☒ Include expiration information in emails sent to signers

Enable document expiration

Check the option to enable document expiration. This will reveal the options you can set for document expiration.

Allow sender to set or modify expiration settings per document

This opens the expiration option on the Send page, to all users in the account. Additionally, they can then adjust the default expiration set.

Allow modification of expiration settings after document is sent

Checking this option will allow users to adjust, extend or remove an expiration for an agreement after it has been sent.

Limit number of days signers will have to sign documents to:

This sets the number of days until the document expires.

Include internal signers when applying document expiration deadlines

If users in your account will be signing or counter-signing agreements, this option will make the expiration apply to them as well as external signers.

Include expiration information in email sent to signers

This adds the expiration date of the transaction in the email sent to the signers.

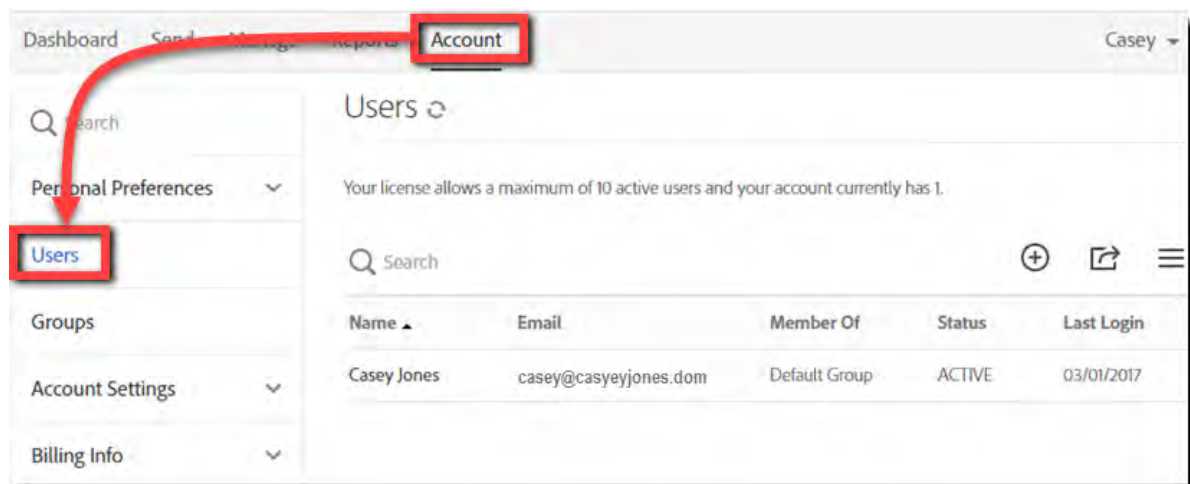
Users and Groups

Users

Users are generally added to an account because they will either be sending out agreements or be group or account level admins. Users that will be signing agreements do not need to be added, unless you want to control their ability to sign with account level settings.

User page features

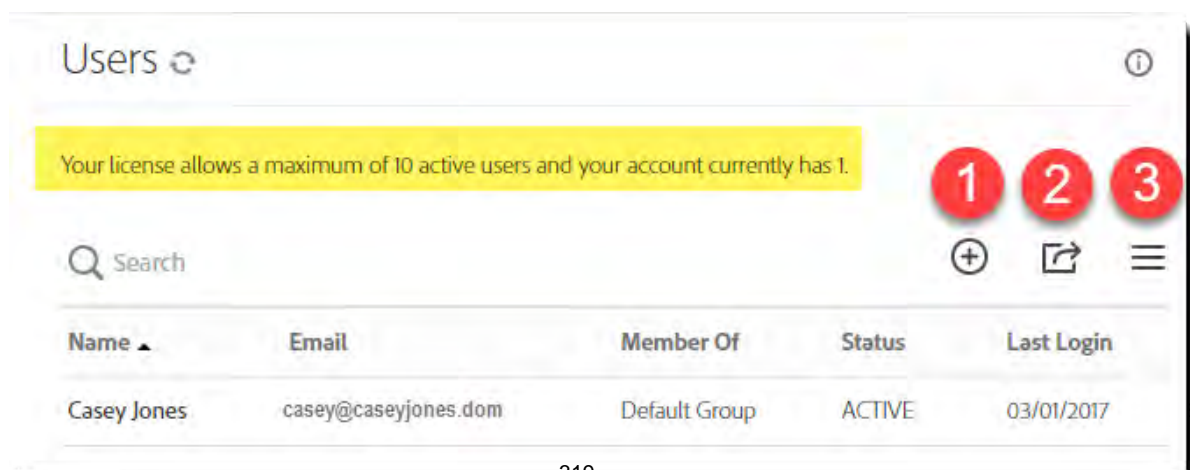
To review or manipulate the users in your account, log in as an Account admin and navigate to: **Account > Users**



At the top of the User page, you will see a short summation of the number of licenses your account allows, and the number of active users consuming those licenses.

If this statement is missing, you have a site license, and can add an unlimited number of users.

The User page has three controls:

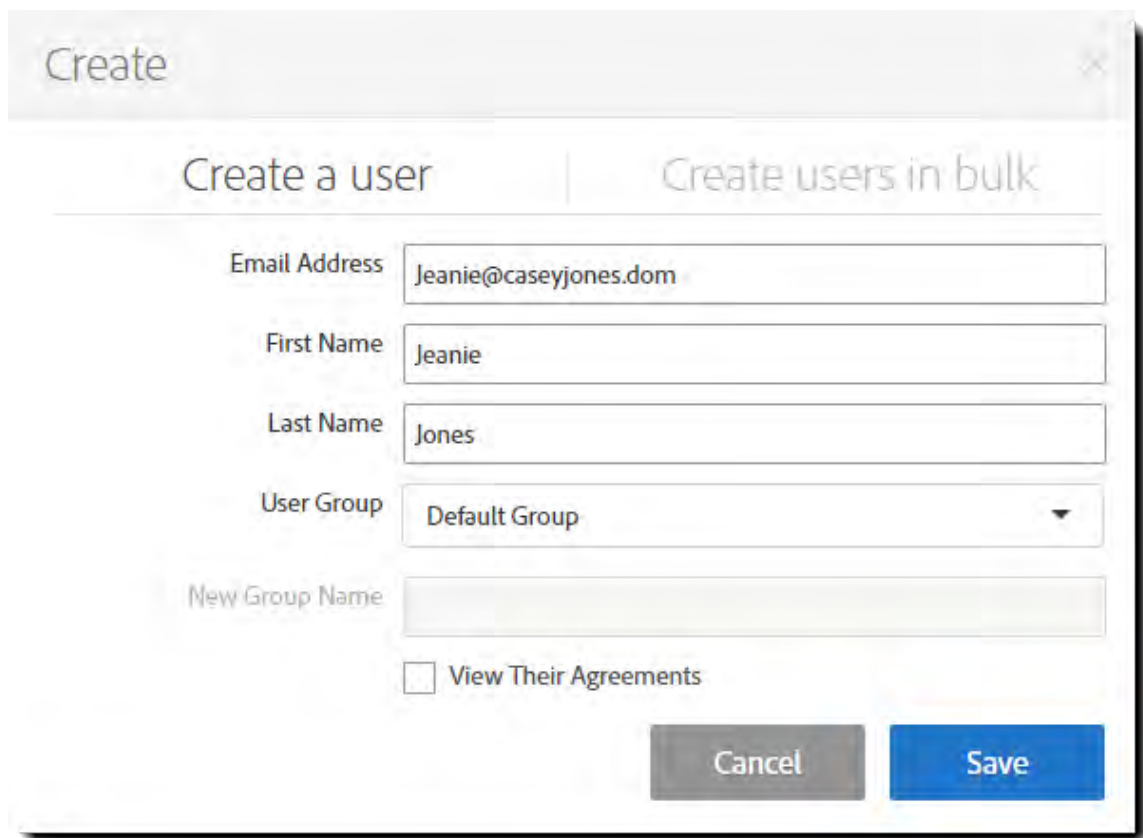


1. **Create a new user** – Opens a pop-up form that will permit you to create a single user, or upload a CSV to create multiple users at one time.
2. **Export user list** – Clicking the Export icon will generate a CSV file that lists all uses in the account, regardless to their status (Active, Created, Inactive or Pending), as well as their personal (account) values (Name, Email, Title, Company, etc.)
3. **Options** – The options list filters what is displayed on the page. By default, only Active users are displayed. You have the option to show All users, or only Inactive users. Further, there are three options for how many users should be shown per page (15, 30 or 50)

How to Create a User

To create a single user:

- Log in as an Account Admin, and navigate to **Account > User**
- Click the “plus” icon to create a new user. The *Create* pop-up will open.



The screenshot shows a 'Create' pop-up window with a close button in the top right corner. It has two tabs: 'Create a user' (selected) and 'Create users in bulk'. The 'Create a user' tab contains the following fields:

- Email Address**: A text input field containing 'Jeanie@caseyjones.dom'.
- First Name**: A text input field containing 'Jeanie'.
- Last Name**: A text input field containing 'Jones'.
- User Group**: A dropdown menu with 'Default Group' selected.
- New Group Name**: A text input field that is currently empty.
- ☐ **View Their Agreements**: A checkbox that is currently unchecked.

At the bottom right of the form are two buttons: a grey 'Cancel' button and a blue 'Save' button.

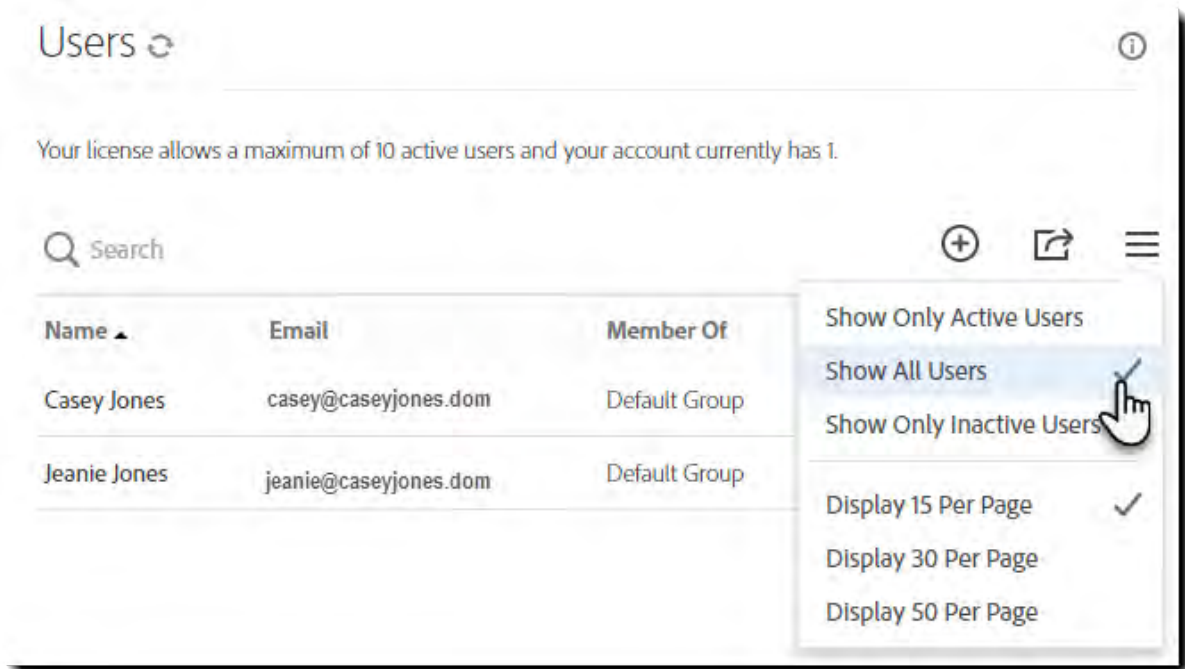
- Enter the email address, first name and last name for the user you want to create. Make sure all this information is correct, especially the email address. Once the user is created the email address cannot be changed until the email entered is verified. If there's an error in the email, it can't be verified.

Check the *View Their Agreements* option if you want to setup a share for this user to yours. This will give you visibility of all the user's agreements.

Once you're done and all the information is correct, click the **Save** button.

You will be returned to the User page.

Click the Options icon and select **Show All Users**



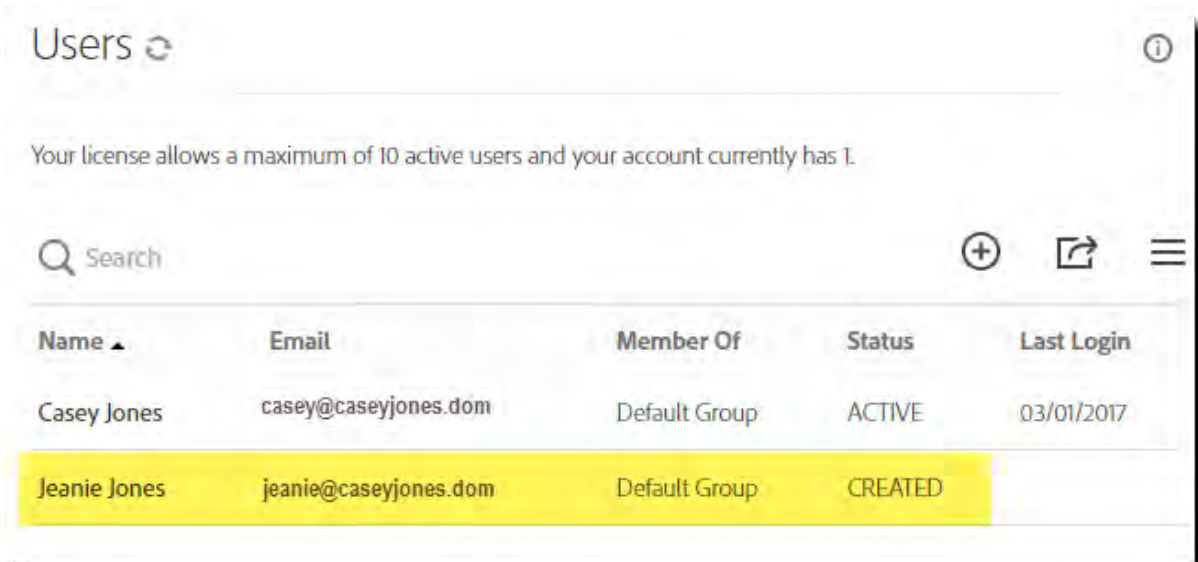
The screenshot shows the 'Users' page with a table of users. A dropdown menu is open, showing options to filter users. A hand cursor is pointing at 'Show All Users'.

Name	Email	Member Of
Casey Jones	casey@caseyjones.dom	Default Group
Jeanie Jones	jeanie@caseyjones.dom	Default Group

- Show Only Active Users
- Show All Users
- Show Only Inactive Users
- Display 15 Per Page
- Display 30 Per Page
- Display 50 Per Page

By showing All Users (vs Only Active Users) you will see the new userID with a *Created* status.

Once the user sets their password, the userID will convert to an *Active* status.



The screenshot shows the 'Users' page with the same table of users. The 'Status' column is now visible, and the 'Last Login' column is also present. The user 'Jeanie Jones' is highlighted in yellow, indicating a 'CREATED' status.

Name	Email	Member Of	Status	Last Login
Casey Jones	casey@caseyjones.dom	Default Group	ACTIVE	03/01/2017
Jeanie Jones	jeanie@caseyjones.dom	Default Group	CREATED	

Note: Adobe Sign users exist in one of five statuses:

- **Active** – A fully enabled userID consuming one license.
- **Inactive** – A fully disabled userID. Inactive users cannot access the Adobe Sign application for any reason, including being a recipient to other agreements.
- **Created** – A userID that has been created by an Admin, but has not yet set their password and activated the userID. Created users do not consume a license.
- **Unverified** - A user that has changed their email address, but has not yet clicked the verification link that was sent to affirm the email change. The account is technically still Active, just locked until the email change is confirmed, so Unverified users consume a license and display in the Show Only Active Users filter
- **Pending** – Pending userIDs are recipients. They have not been created by an admin, do not have passwords, and so they cannot log in. Pending users do not consume a license.

At any time, a Pending userID can be registered and converted to an Active status, and will have a full history of all the Agreements they have ever been party to.

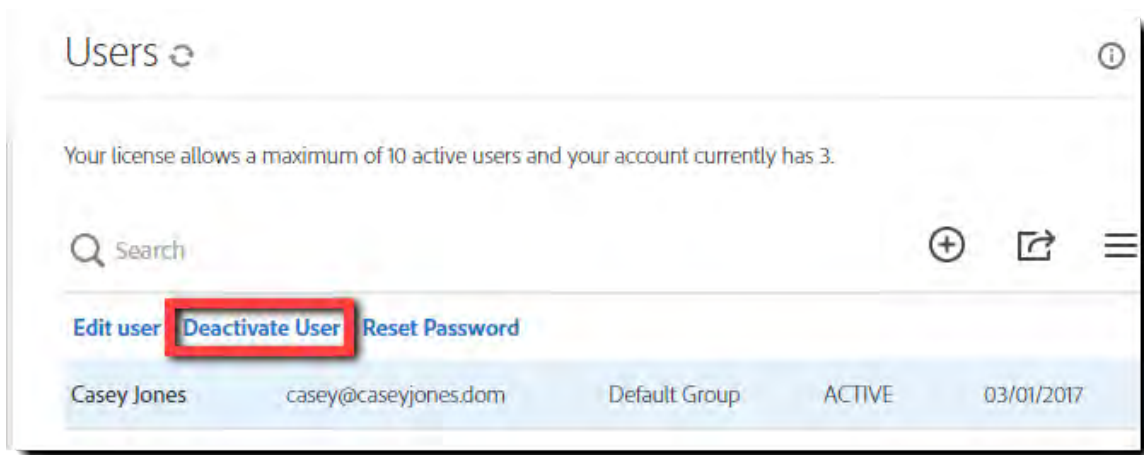
How to Deactivate/Reactivate a user

Deactivating a userID

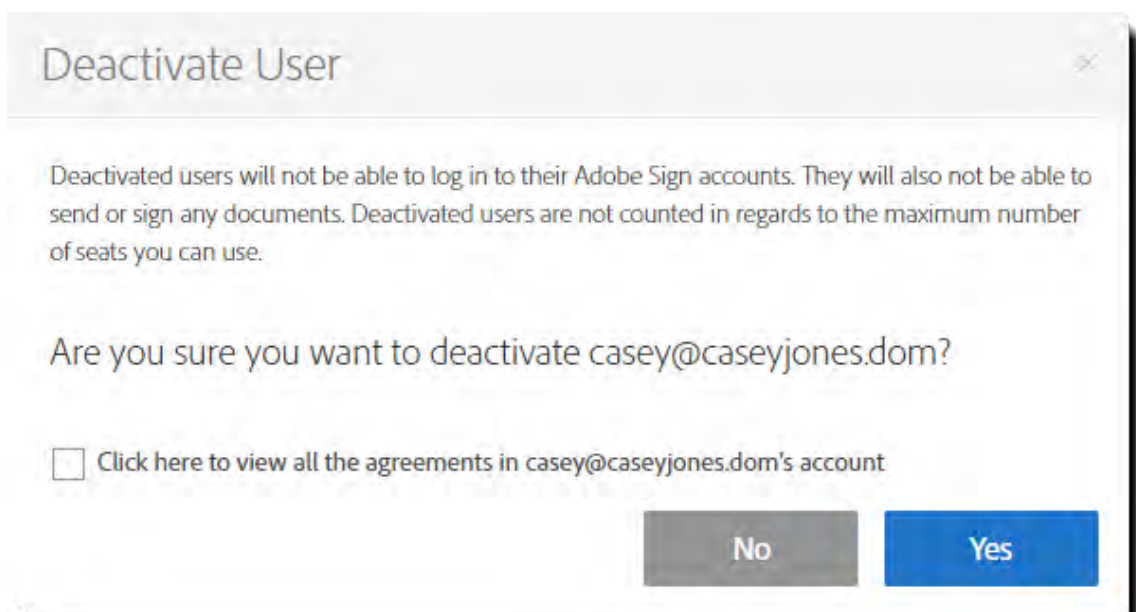
Sometimes the need to deactivate a user may arise. The individual could have left the company and you want to keep that user and related documents secure. As mentioned above, making a user inactive keeps anyone from logging in, sending or signing documents with that userID.

To convert a userID to Inactive:

- Log in as an Admin and navigate to **Account > Users**
- Single click the userID you want to inactivate. The possible actions for the user will appear at the top of the user list



- Click the **Deactivate User** link. This will open the Deactivate User pop-up window



Within the *Deactivate User* pop-up, you have the option to force a share of all agreements to yourself. This is useful if the user being deactivated has content that you may need to recover at a future date.

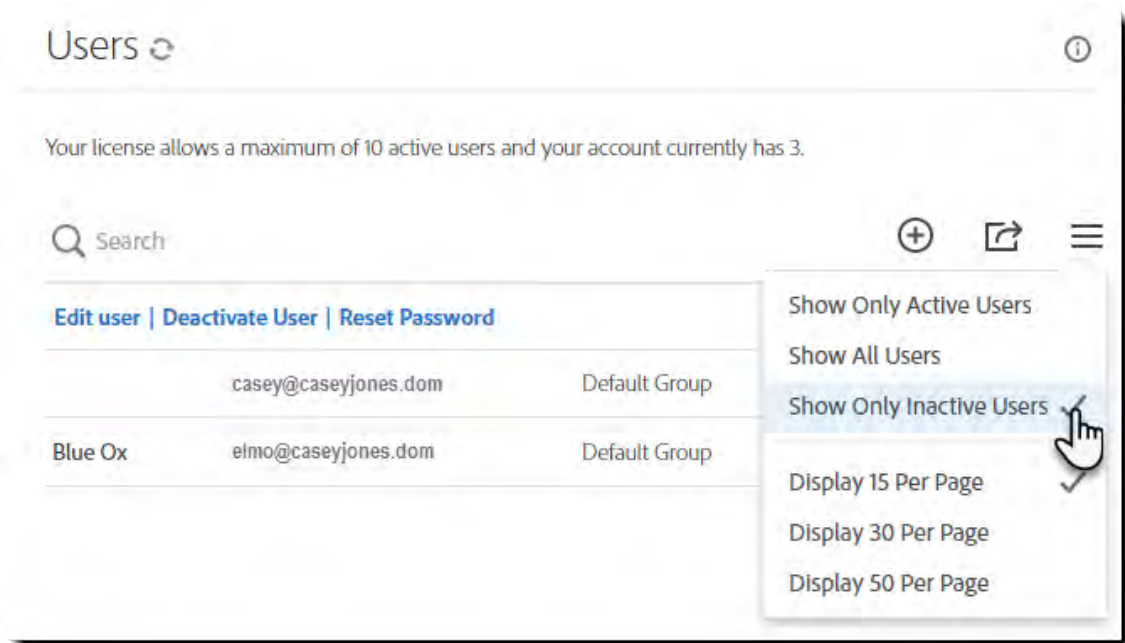
To complete the deactivation process, click the **Yes** button.

The userID will convert to the **Inactive** status and the password for the userID will be voided, making the userID completely inaccessible.

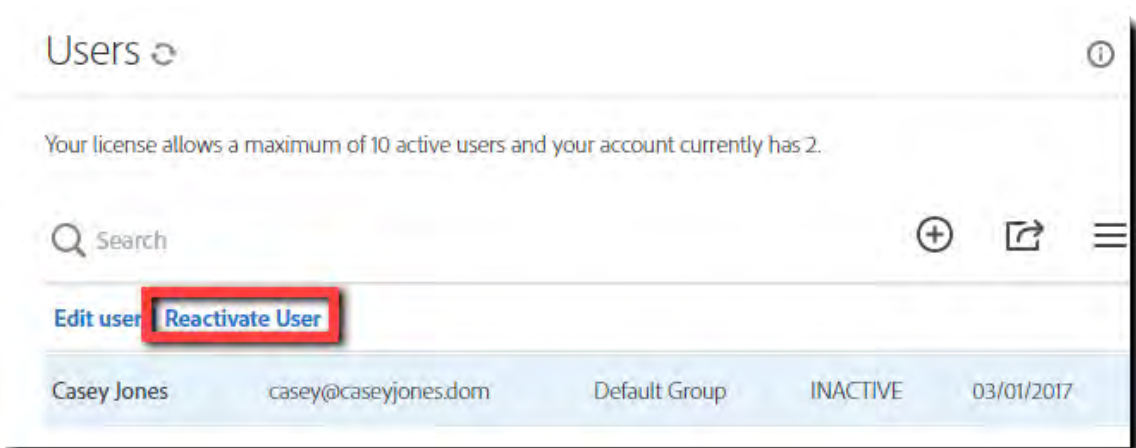
Reactivating a single userID

Reactivating a userID follows the same process as deactivation:

- Log in as an Admin and navigate to **Account > Users**
- Click the **Options** icon and select **Show Only Inactive Users**



- Find the userID you need to reactivate and single click it to expose the links at the top of the user list



- Click the **Reactivate User** link

A green banner should appear indicating you have successfully reactivated the userID.

The reactivated userID converts to an **Active** status, but the password is still expired for the user.

An email will automatically be sent to the user requesting that a new password be installed. Once the password is reset, the user will have full access to all the historic content of the userID.

The user can also use the *I forgot my password* link on the log in page to reset the password.

How to promote a user to admin

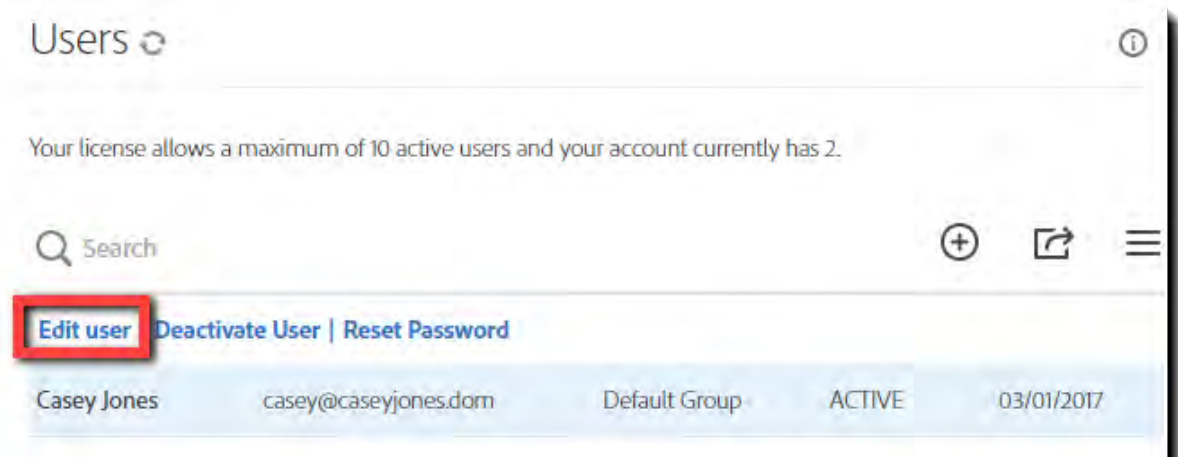
There are three levels of authority in Adobe Sign:

- Users
- Group Administrators
- Account Administrators

All users created individually will be basic Users.

If you need to elevate the authority of any userID, you can do so by:

- Log in to Adobe Sign as an Account admin
- Navigate to **Account > Users**
- Find the userID you want to promote, and select that user to expose the action links at the top of the user list.
- Click the **Edit user** link. This will open the *Edit* pop-up



Edit

Casey Jones
Railroad Man
CaseyJones

Last Login: 03/01/2017 8:40 AM **Email:** casey@caseyjones.com

Status: ACTIVE **Password:** Valid

User Group:
Default Group

☐ User is an account administrator
☐ User is a group administrator
☒ User can sign documents

Auto Delegation
Any agreements sent to casey@caseyjones.com for signature can be automatically delegated to an alternate signer. If you do not want to enable automatic delegation, leave this value blank.

Delegated Signer:

Cancel **Save**

- Within the Edit pop-up window, you have the option to enable the userID as a Group Admin, Account Admin or both. Check the appropriate authority option for the userID
 - Account Admins have full authority within Adobe Sign to edit settings or add users at either the Group or Account level.
 - Group level Admins only have authority within the group they belong to.
- Click **Save** when done.

Note: Adobe Sign does not limit the number of Admins (Account or Group) that can exist within an account. It's possible (but not generally recommended) to promote all userIDs within your account to the Account Admin level.

Creating Users in Bulk

Creating Users in bulk is a process of defining all users in a CSV file, and then uploading that file to Adobe Sign.

Adobe Sign creates all users and immediately sends them emails to set passwords and activate the userIDs.

Note: It's worth pointing out that this process can also be used to [edit the profile values](#) for all the users in your account.

For example, if you have changed your company name, you could export your full user list, edit the value in the Company column, save it, and then upload that CSV back to Adobe Sign. All the userIDs on your CSV will update their Company name values without having to involve the various users.

To create users in Bulk:

- Log in as an Account Admin, and navigate to **Account > User**
- Click the “plus” icon to create a new user. The *Create* pop-up will open
- Click the **Create users in bulk** tab

Create

Create a user | **Create users in bulk**

[Browse...](#) No file has been uploaded

☒ Allow Create Users
☒ Allow Update Users
☒ Allow Create Groups

Create or update many users in batch ([download sample CSV file](#)). [Learn more...](#)

Cancel Import

Note: Three options exist:

- **Allow Create Users** - Deselecting this option only allows you to update existing users. If an e-mail address that is not in your account is provided, no user is created.
- **Allow Update Users** - Deselecting this option only allows you to create users. If an e-mail address of an existing user in your account is provided, the user is not changed.
- **Allow Create Groups** - Deselecting this option keeps you from creating groups. If a nonexistent group name is provided for a user, the group is not created, and the user is put in the Default group instead.

- Click the **download sample CSV file** link. A CSV file will download to your system.
- Open the sample CSV
- Delete the three rows of example data. Leave the first (header) row
- Enter the values needed for the new userIDs you want to create.
 - When creating new users, the required columns are:
 - Email Address
 - First Name
 - Last Name

	A	B	C	D	E	F
1	Email Address	First Name	Last Name			
2	Edgarr@caseyjones.dom	Edgarr	Farindal			
3	Harrgrove@caseyjones.dom	Harrgrove	Mandalick			
4	Sydney@caseyjones.dom	Sydney	McGee			
5						
6						

- Delete any columns you are not using
- Save the CSV (make sure the saved file is still a CSV and not some other format)
- Click the **Browse** button, and select your CSV
- Click **Import** to upload the file

Once the file is imported, Adobe Sign will generate all the userIDs, and a green banner will appear informing you of the number of users created.

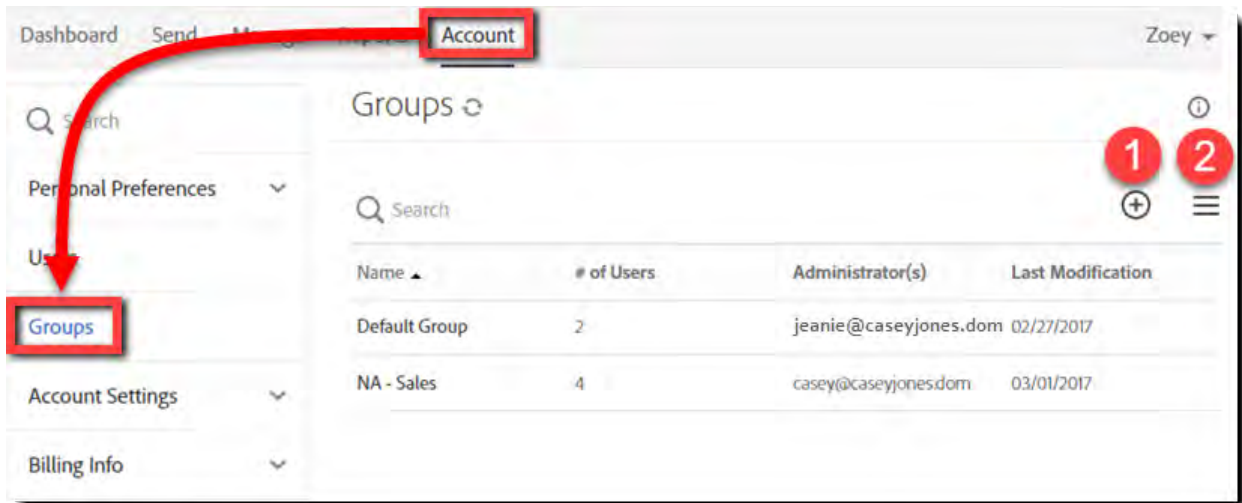
Groups (Business and Enterprise)

Groups allow you to set specific settings for the users inside that group. This means, for example, your sales team can use Adobe Sign differently than your accounting department.

How to Create a Group

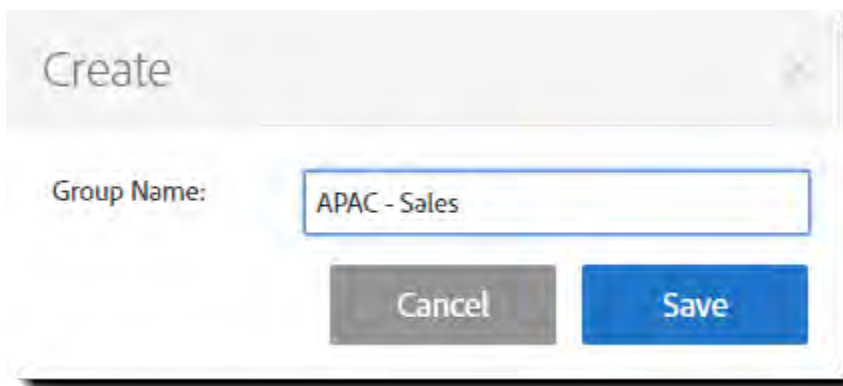
To create a new Group:

- Log in as an Account Admin and navigate to **Account > Groups**

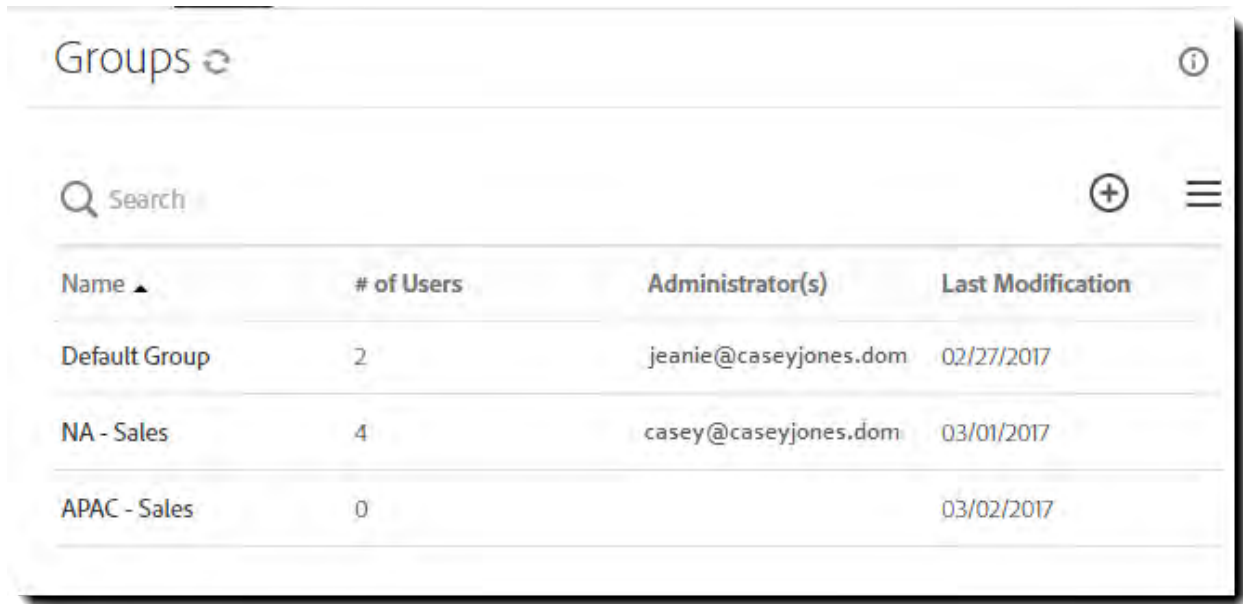


Note: The Groups page has two controls:

1. **Add a new group** - Opens the window to create a new group.
 2. **Options** - Controls how many records (15, 30 or 50) are displayed on the page at any time.
- Click the **Add a new group** icon, and the *Create* window will pop-up requesting the name of the group.



- Enter the name of the Group
- Click **Save**



The screenshot shows the 'Groups' management interface. At the top, there is a search bar and a '+ Add' button. Below is a table with the following data:

Name ▲	# of Users	Administrator(s)	Last Modification
Default Group	2	jeanie@caseyjones.dom	02/27/2017
NA - Sales	4	casey@caseyjones.dom	03/01/2017
APAC - Sales	0		03/02/2017

Once the **Save** button is clicked, the Group is created and will display in the Group list.

How to Add Users to a Group

Once your new group is created, the next step would be to add users to it. Adobe Sign provides three methods, depending on how many users need to be moved:

- Move a single User via the User profile
- Move multiple Users using the *Bulk Create/Edit Users CSV*
- Move multiple Users using the *Assign Users to Group* tool

Moving a single User via the User profile

To assign a single User to a Group:

- Log in as an Admin and navigate to **Account > Users**
- Double click the specific userID you want to edit. This opens the User info panel
- Click the **User Group** drop-down box to expose the options
- Select the group the User is to be assigned to
- Click **Save**

Edit

Casey Jones

Railroad Man

CaseyJones

Last Login: 03/01/2017 8:40 AM

Email casey@caseyjones.dom

Status: ACTIVE

Password Valid

User Group:

NA - Sales

APAC - Sales

Default Group

NA - Sales

☒ User is an account administrator

☒ User is a group administrator

☒ User can send documents

☒ User can sign documents

Any agreements sent to casey@caseyjones.dom for signature can be automatically delegated to an alternate signer. If you do not want to enable automatic delegation, leave this value blank.

Delegated Signer:

Cancel

Save

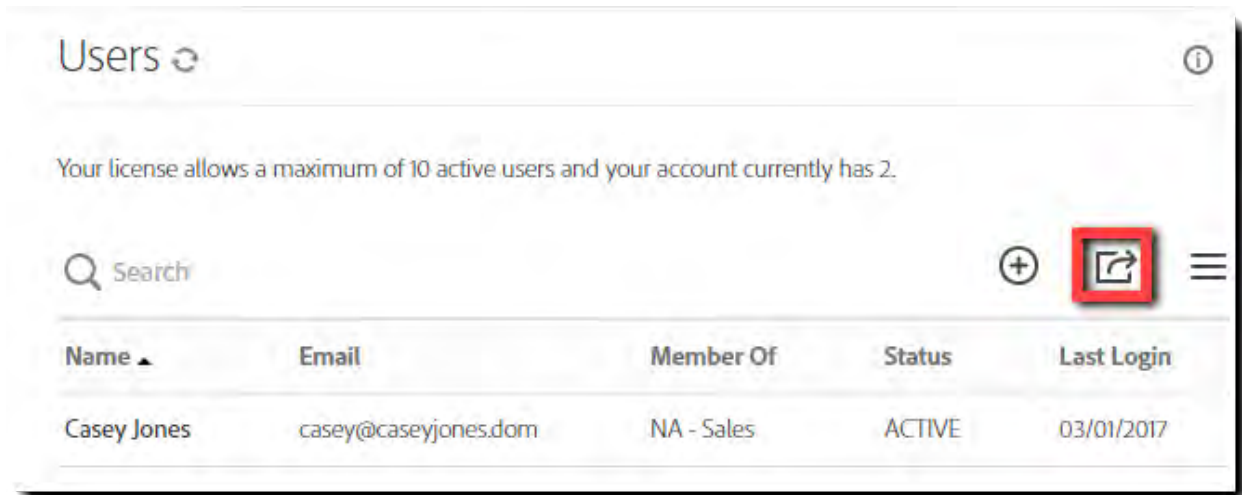
Moving multiple Users using Bulk User Edit

The *Create Users in Bulk* feature can also be used to edit existing users.

This method tends to be better when you have multiple values you need to change in addition to just the Group setting, but if you are fully restructuring, bulk update may be the way to go.

To update your User Groups via Bulk Update:

- Log in as an Admin, and navigate to **Account > Users**
- Click the **Export user list** icon. A CSV will download to your system with the full list of users in your account



- Open the downloaded CSV, and delete any columns you are not going to use
 - In the case of simply assigning users to groups, you only need:
 - Email Address
 - First Name
 - Last Name
 - Group Name
- Delete any rows of Users that you do not need to update
- **Save** the CSV (Make sure that the format remains CSV)

	A	B	C	D	E	F	G
1	Email Address	First Name	Last Name	Group Name			
2	blue@caseyjones.dom	Blue	Ox	APAC - Sales			
3	casey@caseyjones.dom	Casey	Jones	APAC - Sales			
4	jeanie@caseyjones.dom	Jeanie	Jones	APAC - Sales			
5	elmo@caseyjones.dom	Elmo	Kappernic	APAC - Sales			
6	hester@caseyjones.dom	Hester	Mackladang	APAC - Sales			
7							

- Click the “plus” icon to create a new user. The Create pop-up will open
- Click the **Create users in bulk** tab
- Browse to select the CSV file you just saved
- Click **Import**

Create

Create a user Create users in bulk

Browse... GroupUpdate.csv

Clear

☐ Allow Create Users
☒ Allow Update Users
☒ Allow Create Groups

Create or update many users in batch ([download sample CSV file](#)). [Learn more...](#)

Cancel Import

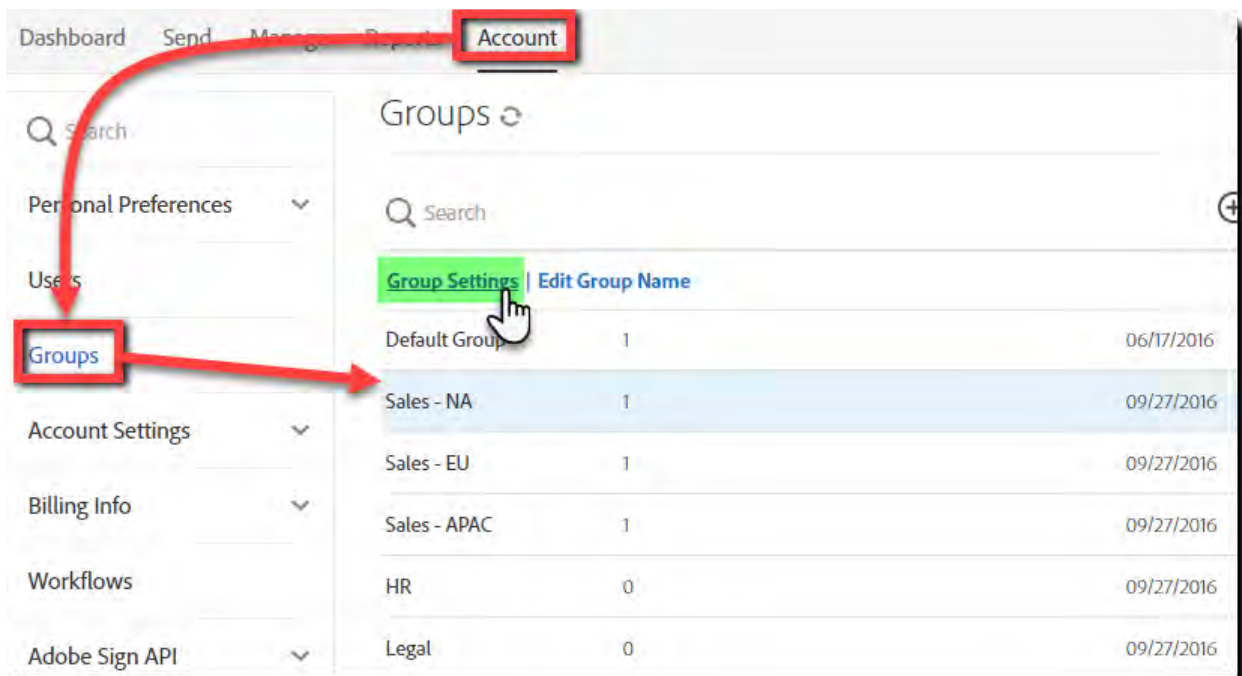
Once the Import button is clicked, the users will be updated in the system with the new values on the CSV. A green banner will appear at the top of the page to indicate how many users were updated.

Assign Users to Group from within the Group Settings

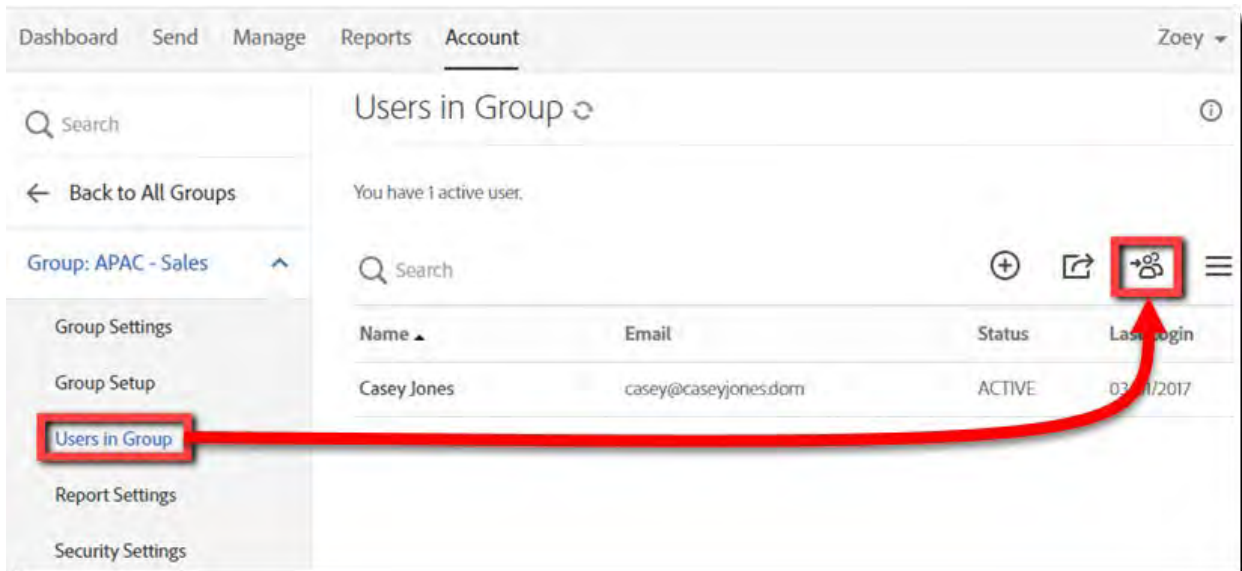
When you need to move multiple users to a new group, but the scope of the move isn't large enough to warrant using Bulk User Edit, the best option is to use the Assign Users to Group option within the Group settings.

To access the *Assign Users to Group* feature:

- Log in as an Account Admin and navigate to **Account > Groups**
- Double-click the group you want to move users into. This opens the Group level settings
 - You can also single click the group to select it, and then click the **Group Settings** link



- Click the **Users in Group** option on the left rail
- Click the **Add users to group** icon



The Assign Users to this Group window will open, showing all the Active Users that are not currently assigned to this group.

- Click the **Options** icon, and select **Show All Users**

Assign Users to this Group

Search

Name ▲	Email	Member Of	Stat
	elmo@caseyjones.dom	NA - Sales	PEN
Blue Ox	blue@caseyjones.dom	NA - Sales	CRE
Jeanie Jones	jeanie@caseyjones.dom	Default Group	INA
Zoey Jones	zoey@caseyjones.dom	Default Group	ACT

Show Only Active Users
 Show All Users ✓
 Show Only Inactive Users
 Display 5 Per Page ✓
 Display 10 Per Page
 Display 25 Per Page
 Display 50 Per Page

Selected Users

Cancel

Assign

- Double click any User you want to move to the Group. The selected users will populate in the *Selected Users* field at the bottom of the window.
 - To remove a user from the *Selected Users* field, click the X next to the email
- Once all users are selected, click the **Assign** button

Assign Users to this Group

Search

Select User

	elmo@caseyjones.dom	NA - Sales	PENDING
Zoey Jones	zoey@caseyjones.dom	Default Group	ACTIVE 03/02/2017

Selected Users

jeanie@caseyjones.d X

blue@caseyjones.dom X

Cancel

Assign

Group level Admin authority controls

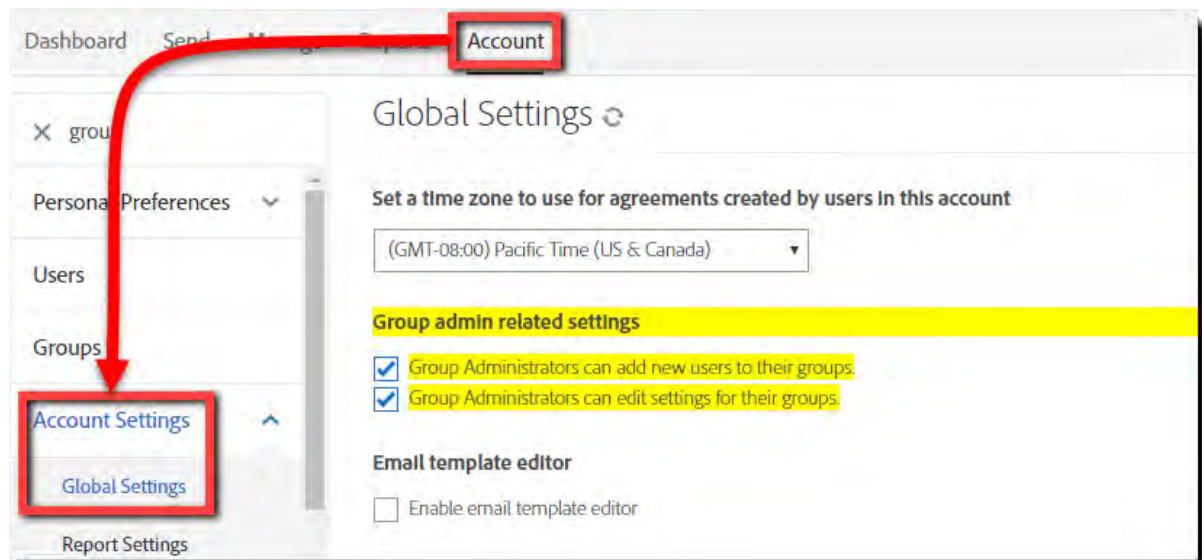
Account level Administrators can define the scope of the Group Administrators authority via three settings:

- Group Administrators can add new users to their groups.
- Group Administrators can edit settings for their groups.
- What report data can group admins see?

These settings are ubiquitous for all group admins, and offer no deeper granularity. If you disable the ability for Group Admins to add users, that will apply to all Group Admins within the Account.

To adjust the first two settings:

Log in as an Account Admin and navigate to **Account > Account Settings > Global Settings > Group Admin Related Settings**



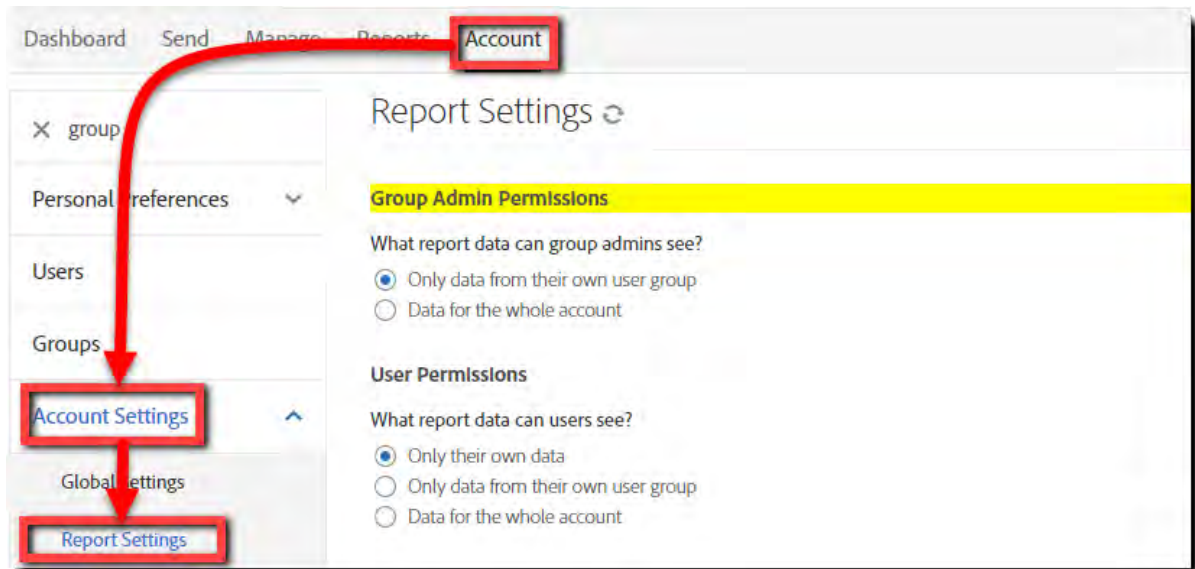
Enabling **Group Administrators can add new users to their groups** will grant any Group Admin the authority to add any user to their group with all normal restrictions applied.

Normal restrictions include situations like:

- The user is in another Group/Account
- The user's email domain is not an approved domain for the account

Enabling **Group Administrators can edit settings for their groups** allows the Group admin to over-ride the Account level settings for their group.

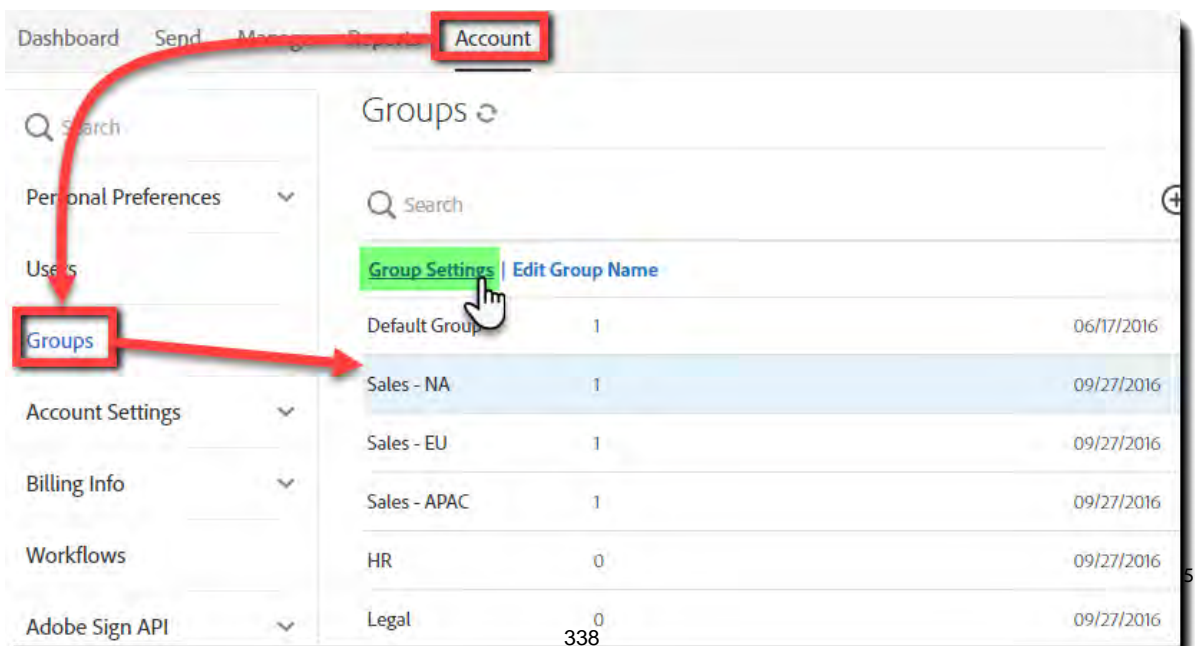
To edit the **What report data can group admins see?** setting, navigate to **Account > Account Settings > Report Settings**



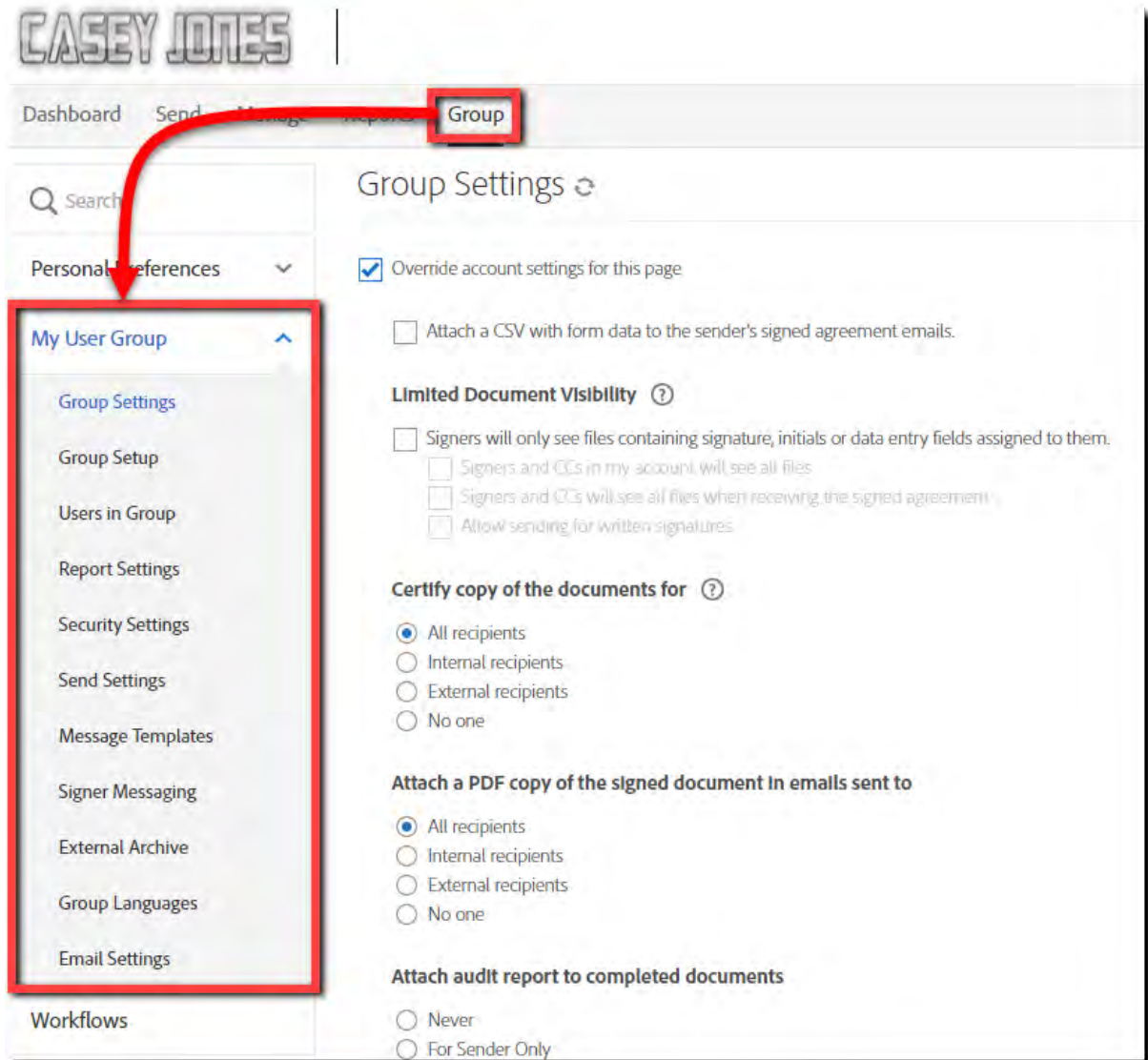
Adjusting Group level settings

All groups will inherit the account level settings by default. However, it is possible to override most of the account level settings at the group level. This is particularly valuable if you have select users in need of special recipient roles, recipient validation methods, or even unique branding.

Account admins will navigate to **Account > Groups**, and then double click the Group to open the group level settings, or single click the group and select **Group Settings** from the link options at the top of the list.



If Group level admins have been given the authority to change Group level settings, they only need to click the **Group** link at the top of the page to open the settings.



All of the settings presented to group admins are the same as the account level settings and function in the same way.

Library Templates

A library template is a reusable document object. Adobe Sign supports two types of library templates: document templates and form field templates.

- **Document Templates**—A document template is a reusable document. Document templates can be shared with other users in your account, allowing multiple users to send out the same document without needing to make any changes.
- **Form Field Templates**—A form field template is a reusable field layer that can be applied to any document. Form field templates can also be shared with other users in your account. Form field templates are ideal in the following situations:
 - You have one field layout that works for multiple documents.
 - You have a document that can be sent several different ways.
 - You need to revise document's content, but the fields remain in the same place.

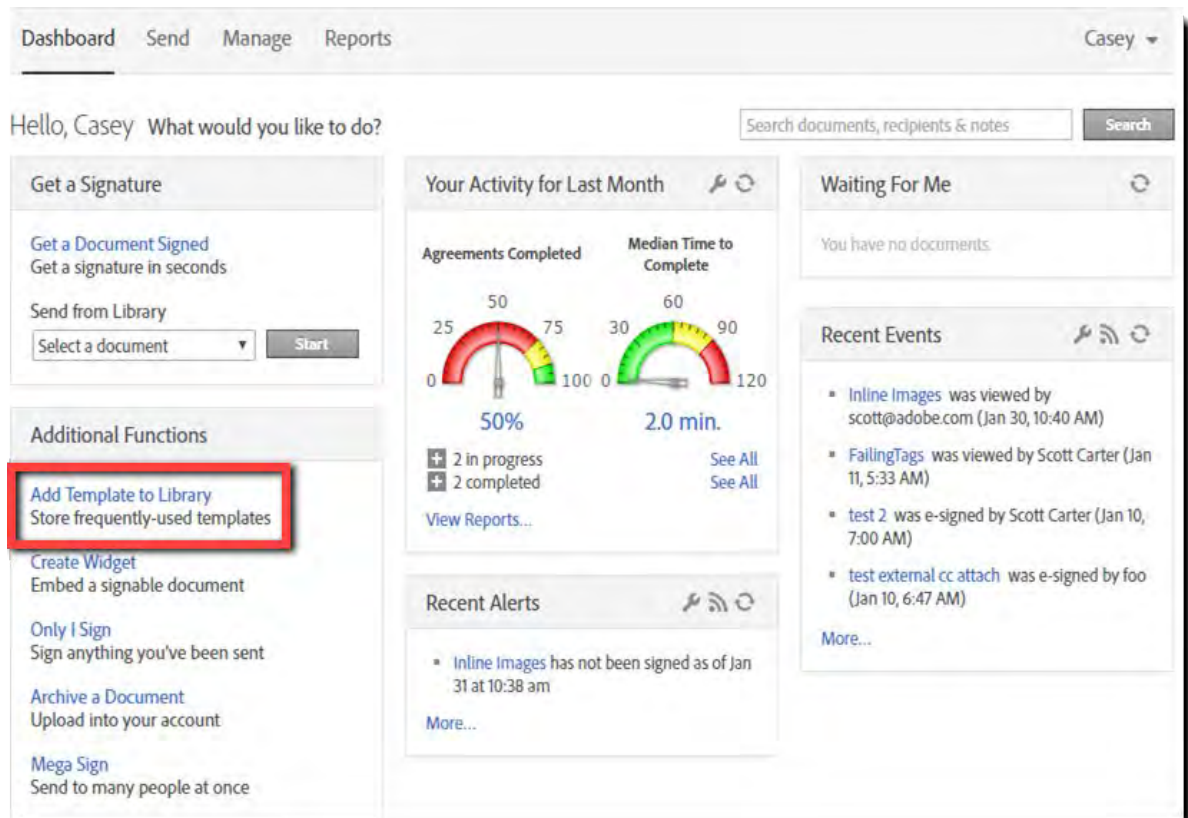
Instead of creating a new library document every time a document is updated, the same form field layer can be applied. Form field templates can be edited to facilitate changes in the arrangement of fields or field properties. Again, all the tools in the authoring environment are available when creating a form field template.

As a best practice, a single user (Document Administrator) should be responsible for creating and maintaining templates. Creating a Doc Admin userID eliminates confusion as to what templates to use and provides version control for your reusable documents.

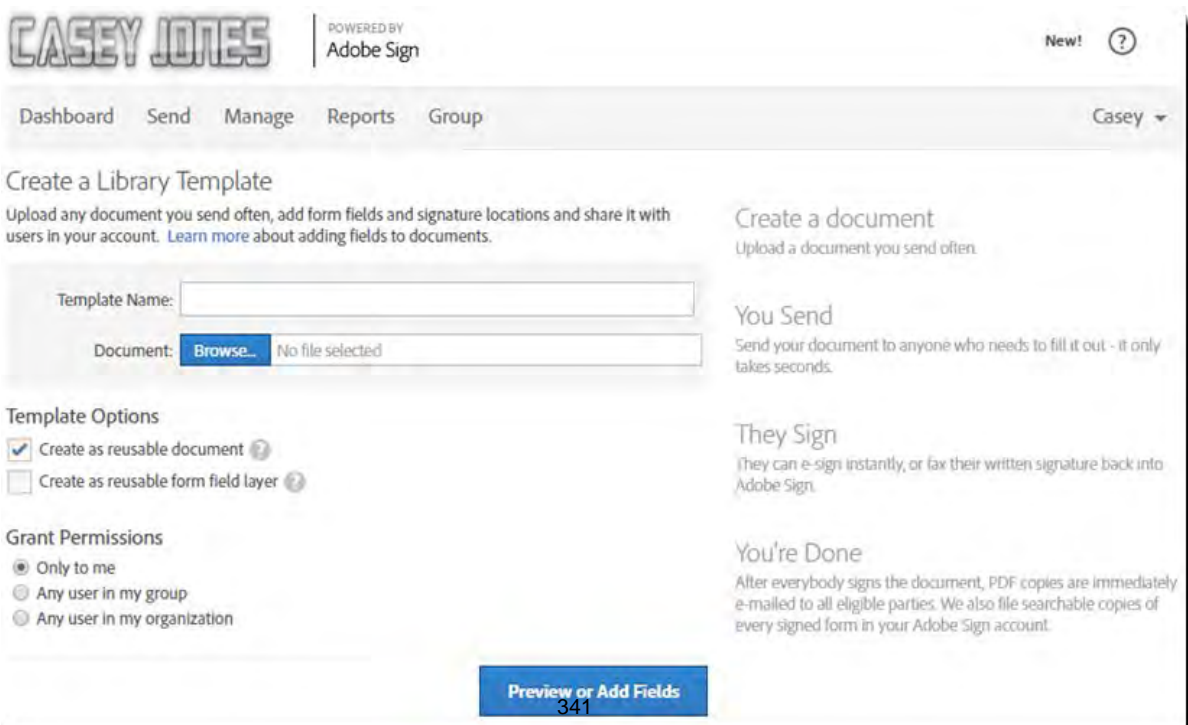
We recommend using a distribution list or functional email for the Doc Admin user login. This allows you to control access to this Doc Admin login while at the same time allowing the responsibility to be shared as needed.

Creating a Reusable Document

1. Click the **Dashboard** tab. Then, in the *Additional Functions* panel, click **Add Template to Library**.



The *Create a Library Template* page displays:



2. In the *Template Name* field, enter a name for your template. This can be changed later if necessary.
3. Click the **Browse** button to navigate to the file on your local system to be used to create your reusable template. If you are creating a reusable document, this file and its content will be used. If you are creating a reusable form field layer, the content of the file will not be included in the template.
4. Select the appropriate Template Option, either *Create as reusable document*, *Create as a reusable form field layer*, or both.

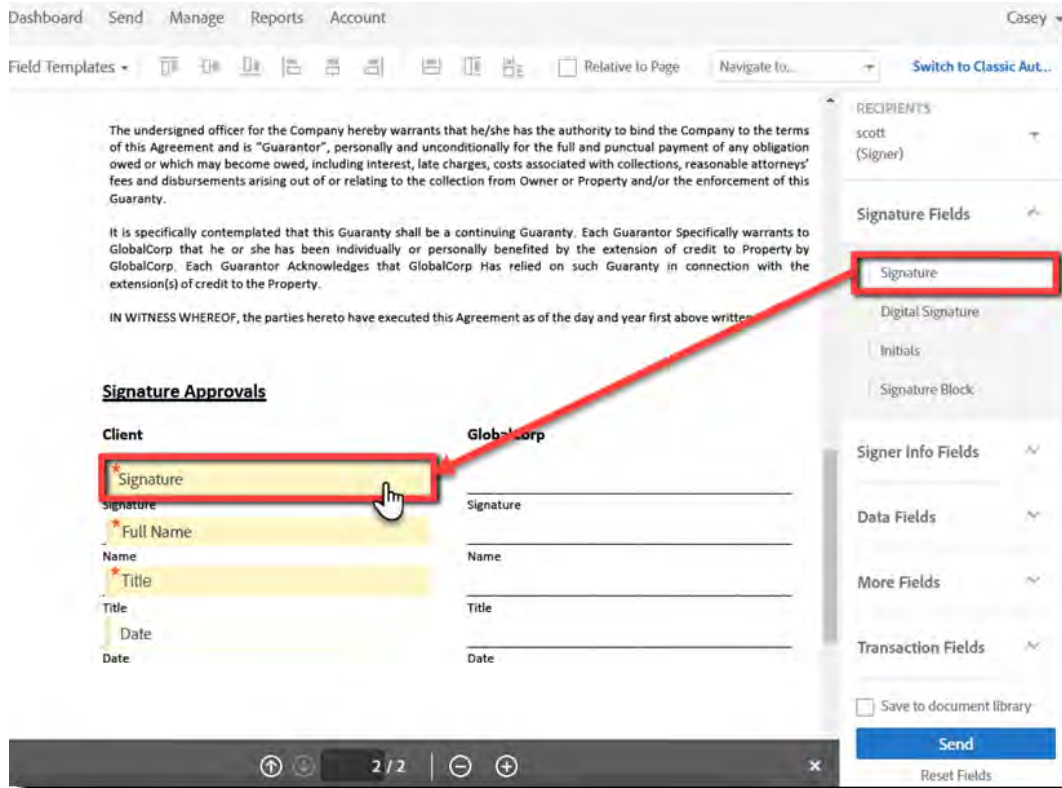


5. Select the appropriate permissions option for sharing the template. When building and testing a new template, it is recommended that you set the permissions to just yourself, and then expand access once you are satisfied the document is working as intended.



Note: Group permissions can only be granted to the group you are currently in. You cannot grant permissions to other groups.

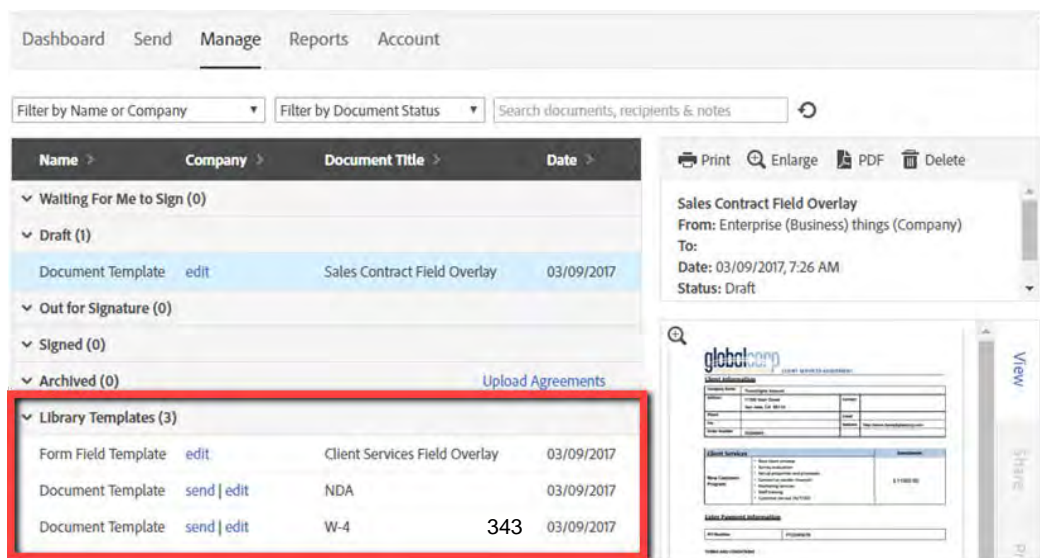
6. Click the **Preview or Add Fields** button. The *Authoring experience* displays.



7. Place the required fields that are for the intended participants by dragging them from the form fields tabs and dropping them onto the document.
8. When you're done adding fields, click the **Save** button.

The template will now display under the Library Templates section of your Manage page. If you have shared the template with users in your group or in your organization by granting permission, the template now also displays in the Library Templates section of their Manage pages, and they can use it to send as often as they like.

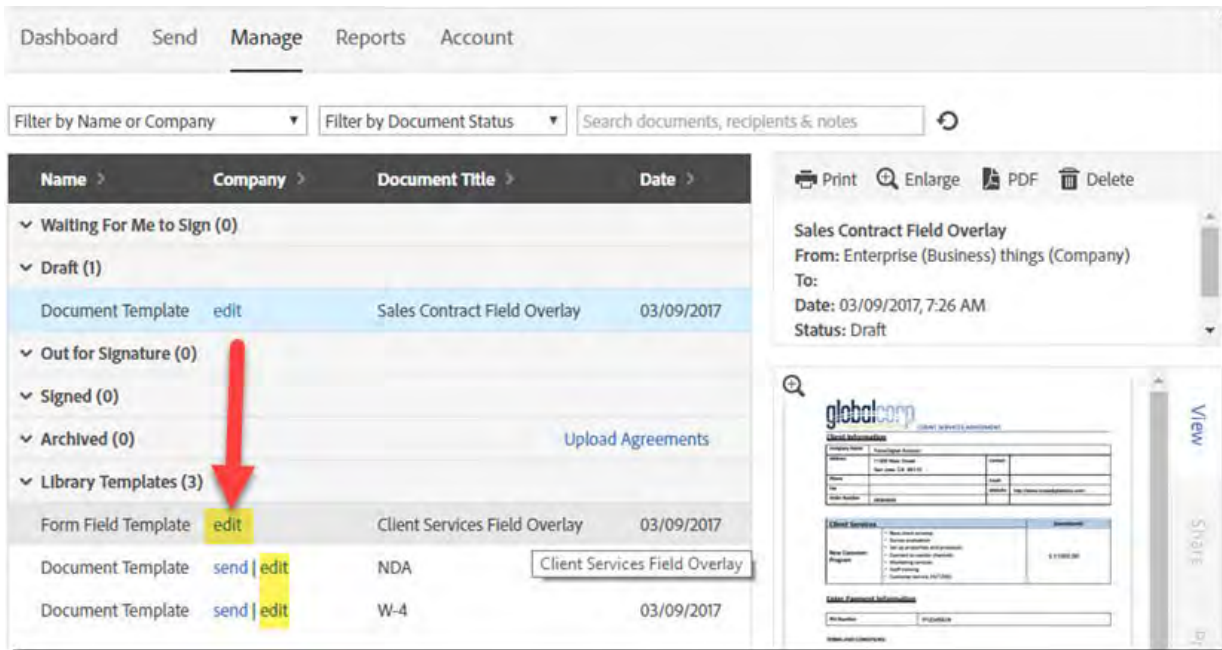
Note: Only the user who created the library template can edit it or delete it.



Editing Template Permissions

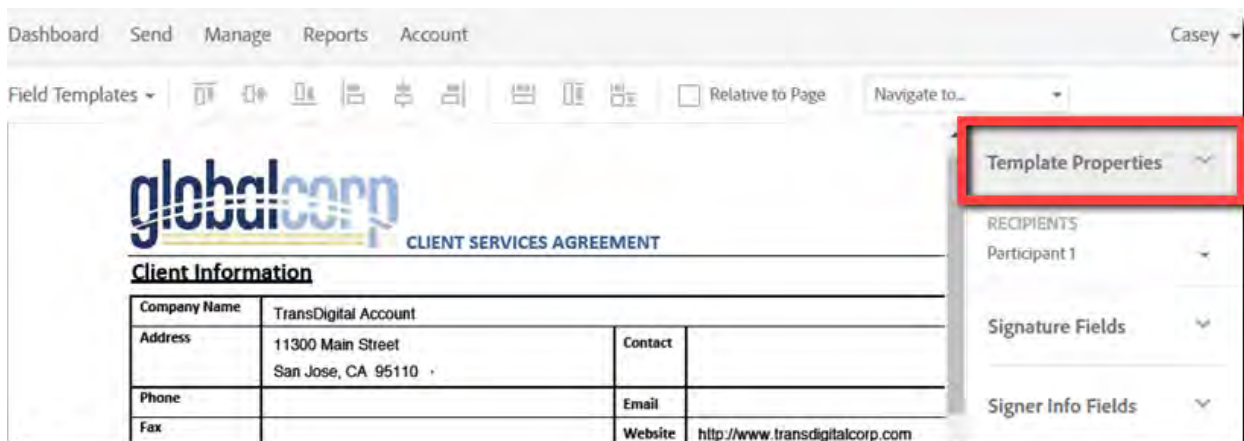
The access permissions for any template can be edited by the **creator** of the template. To do so:

- Log in as the template owner
- Navigating to the **Manage** page
- Find the template to be edited and clicking the **edit** link



This will open the template in the Authoring environment.

At the top of the right rail, you will see **Template Properties**.



Click the Template Properties header to expand the section and you will see the available options:

- **Template Name** – You can readily change the template name at any time.
- **Template Type** – At any time you can convert the available template to make it available as a document, form field overlay, or both
- **Who can use** – This setting dictates which users will have access to the template.

The screenshot shows the Adobe Sign interface. The top navigation bar includes 'Dashboard', 'Send', 'Manage', 'Reports', and 'Account'. The user 'Casey' is logged in. The document is titled 'GlobalCorp Client Services Agreement'. The 'Template Properties' panel is expanded on the right, showing the following settings:

- TEMPLATE NAME:** GlobalCorp Client Services Agreement
- TEMPLATE TYPE:** ☒ Both (Other options: Reusable document, Reusable form field layer)
- WHO CAN USE:** ☒ Only me (Other options: Any user in my group, Any user in my organization)
- RECIPIENTS:** Participant 1

The main document content includes a 'Client Information' section with a table for company details and a 'Client Services' section with a table for services and investment.

Client Information	
Company Name	TransDigital Account
Address	11300 Main Street San Jose, CA 95110
Phone	
Fax	
Order Number	28384945

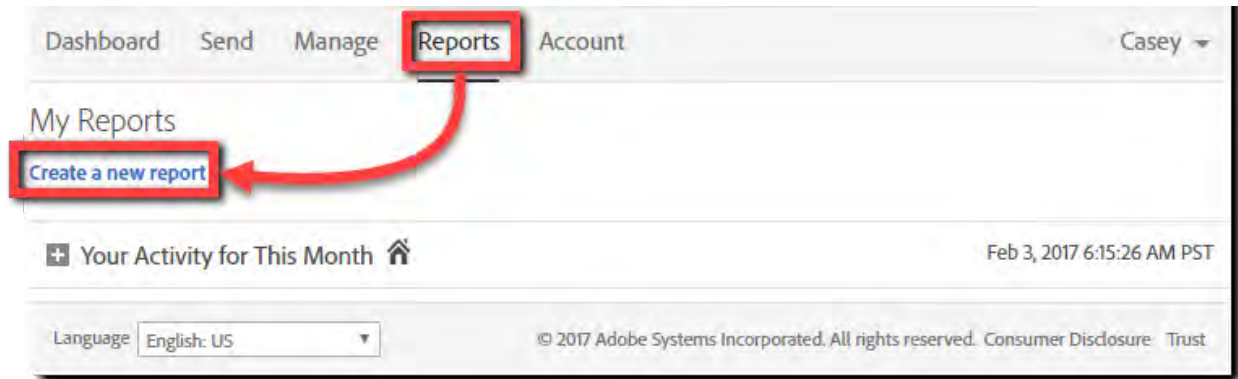
Client Services	Investment
New Customer Program <ul style="list-style-type: none">New client onrampSurvey evaluationSet up properties and processesConnect to vendor channelsMarketing servicesStaff training	\$ 11000.00

Note: You can only share a document to the Group your userID is a member of. If you are authenticated as an Account admin, make sure to move your userID to the correct group before changing the template properties from "Only Me" to "Any user in my group".

Reports (Adobe Sign – Business and Enterprise)

The report feature lets you check on how your account is using Adobe Sign. Build your own reports and gain complete visibility into your document signing process, while seeing how individual groups or users are doing.

To create a new report, navigate to the Reports page by clicking the Reports tab, then click on the **Create a new report** link.



The *Create a New Report* page displays:

The screenshot shows the 'Create a New Report' page in the Adobe Sign Admin Guide. The page has a top navigation bar with 'Dashboard', 'Send', 'Manage', 'Reports' (selected), and 'Account'. A user profile 'Casey' is in the top right. The main heading is 'Create a New Report'. The page is divided into sections on the left and right. The left section has a grey background and lists categories: 'Creation Date', 'Users & Groups', 'Workflows & Documents', 'Document Name', 'Mega Sign', 'Performance Goals', 'Benchmark', 'Graph Agreements By', and 'Et Cetera'. The right section contains the corresponding configuration options. 'Creation Date' has radio buttons for 'This Week', 'Last Week' (selected), 'This Month', 'Last Month', and 'Date Range'. 'Users & Groups' has radio buttons for 'All Users' (selected), 'Filter by User', and 'Filter by Group'. 'Workflows & Documents' has radio buttons for 'All Workflows & Documents' (selected), 'Filter by Workflow', and 'Filter by document'. 'Document Name' has a dropdown menu set to 'contains' and an adjacent text input field. 'Mega Sign' has a checkbox for 'Include MegaSign Agreements'. 'Performance Goals' has a heading 'Set your performance goals by specifying thresholds for gauge colors:' followed by two rows of settings: '% Completed' and 'Time to Complete', each with 'Green' and 'Yellow' thresholds. 'Benchmark' has a message: 'Benchmarking is not enabled for your account. You can opt-in and enable it on the [report settings](#) page.' 'Graph Agreements By' has checkboxes for 'Date', 'Sender', 'Group', 'Form', 'Workflow', and 'Signature Type', all of which are checked. 'Et Cetera' has three settings: 'Animation' (radio buttons for 'Yes' (selected) and 'No'), 'Color Shading' (radio buttons for 'Yes' (selected) and 'No'), and 'Bar Charts' (radio buttons for '3D' (selected) and '2D'). At the bottom right are two buttons: 'Run Report' (blue) and 'Cancel' (grey).

Dashboard Send Manage **Reports** Account Casey ▾

Create a New Report

Creation Date ☐ This Week ☒ Last Week ☐ This Month ☐ Last Month ☐ Date Range

Users & Groups ☒ All Users ☐ Filter by User ☐ Filter by Group

Workflows & Documents ☒ All Workflows & Documents ☐ Filter by Workflow ☐ Filter by document

Document Name contains ▾

Mega Sign ☐ Include MegaSign Agreements

Performance Goals Set your performance goals by specifying thresholds for gauge colors:

% Completed: Green: > % Yellow: > %

Time to Complete: Green: < Min. Yellow: < Min.

Benchmark Benchmarking is not enabled for your account. You can opt-in and enable it on the [report settings](#) page.

Graph Agreements By ☒ Date ☒ Sender ☒ Group ☒ Form ☒ Workflow ☒ Signature Type

Et Cetera Animation: ☒ Yes ☐ No Color Shading: ☒ Yes ☐ No Bar Charts: ☒ 3D ☐ 2D

Run Report **Cancel**

Report Parameters

When setting up a report, multiple parameters can be set to customize the results. All the parameters described below are available.

Creation Date

The creation date is the time frame you want the report to encompass. This can be one of the four predetermined time frames (this week, last week, this month, last month) or enter a custom date range.

The screenshot shows the 'Creation Date' parameter interface. It includes five radio buttons: 'This Week', 'Last Week', 'This Month', 'Last Month', and 'Date Range'. The 'Date Range' option is selected. Below the radio buttons, there is a 'From' field containing '06/23/1912' and a 'to' field. A calendar widget is open, showing the month of June, 1912. The calendar has a header with navigation arrows and the text 'Today'. The days of the week are listed as Sun, Mon, Tue, Wed, Thu, Fri, Sat. The dates 1 through 30 are displayed in a grid. The date 23 is highlighted. At the bottom of the calendar, it says 'Select a date'.

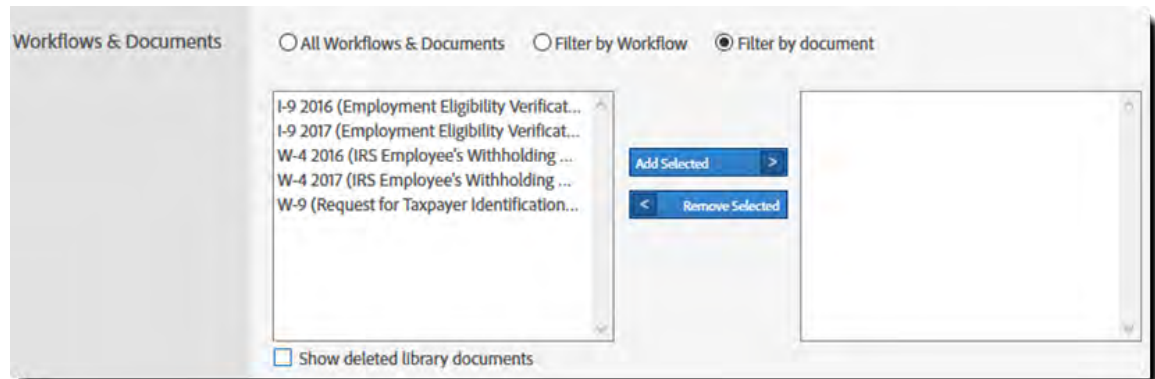
Users & Groups

This parameter lets you run the report on specific users or groups. One or more can be chosen for either, or you can run the report against all users in the account.

The screenshot shows the 'Users & Groups' parameter interface. It includes three radio buttons: 'All Users', 'Filter by User', and 'Filter by Group'. The 'Filter by Group' option is selected. Below the radio buttons, there is a list of groups: 'Default Group', 'HR', 'Legal', 'Sales - APAC', 'Sales - EU', and 'Sales - NA'. To the right of this list are two buttons: 'Add Selected' and 'Remove Selected'. To the right of these buttons is an empty list box for the selected groups.

Documents & Workflows

Specific documents can be chosen to include in the report with this option. The documents listed in this field are the library documents used throughout the account. Individual, one-off documents will not be listed here.



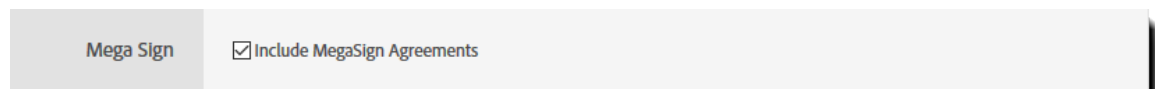
Document Name

This parameter is used to include or exclude documents that contain or do not contain a given variable. You can choose to include or not include the string entered.



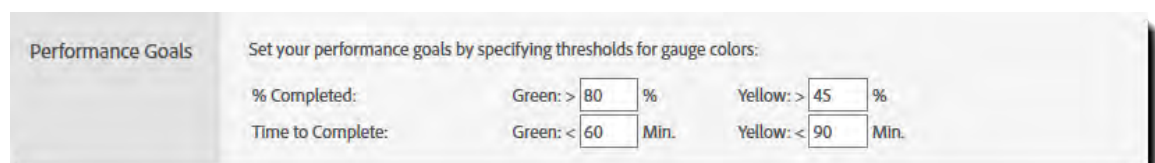
Mega Sign

Enabling this parameter includes Mega Sign agreements in the resulting report



Performance Goals

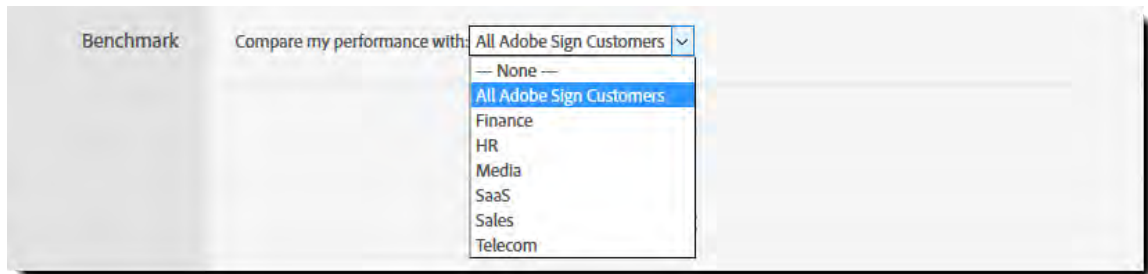
You can set thresholds for performance, using the Performance Goal view. The gauges reflecting performance are displayed in the resulting report.



Benchmark

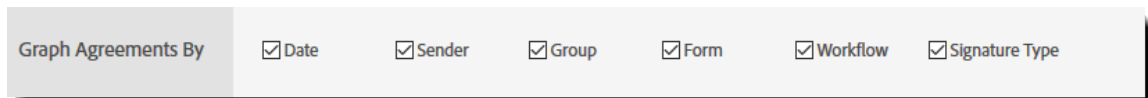
By default, the benchmark parameter is disabled for reports. Click the report settings link to enable it.

Benchmarking provides an expanded method for keeping track of agreement progress and signing rates.



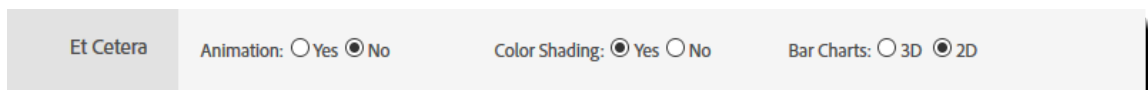
Graph Agreements By

Each enabled option (by Date, Sender, Group, Form, Workflow, and Signature Type) provide a different type of graph on the report.



Et Cetera

The parameters in this section are for altering the graphics on the resulting report. Changing these from the default parameters can speed up the report process.

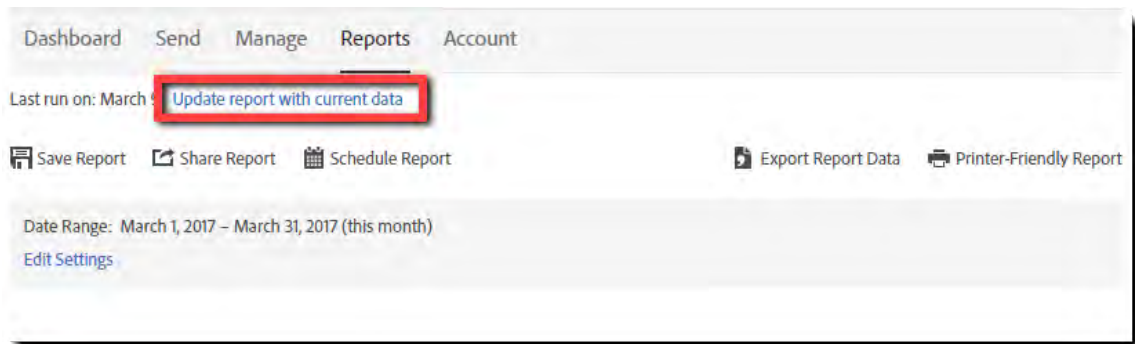


Report Results

Once you click the **Run Report** button, the report will be generated based on your parameters. There are multiple actions you can take with your report.

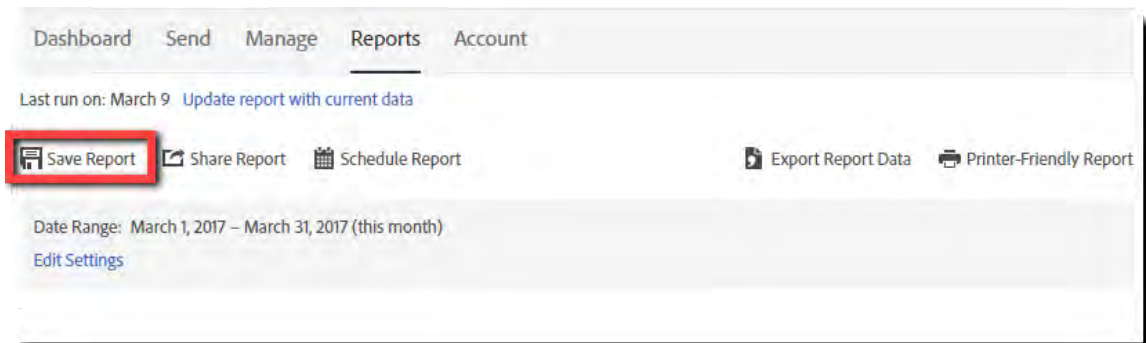
Update Report with Current Data

Clicking this link is like refreshing the page. The new report will include recent transactions and activity.



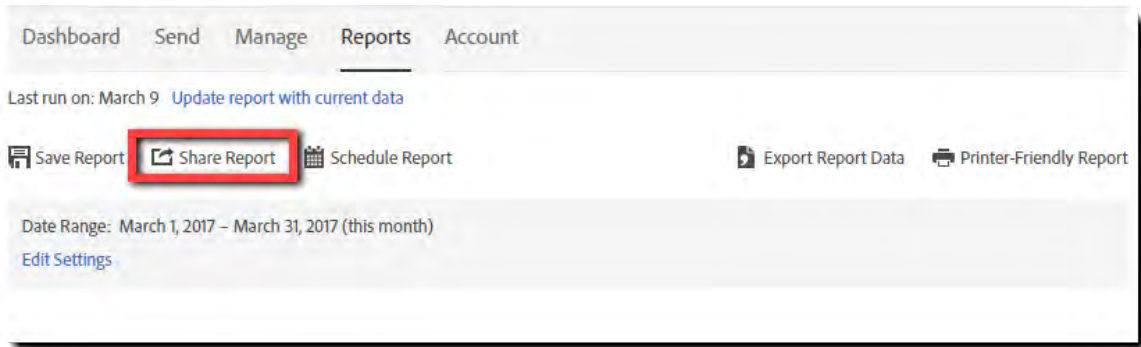
Save Report

Saving the report allows you to run this report again in the future.



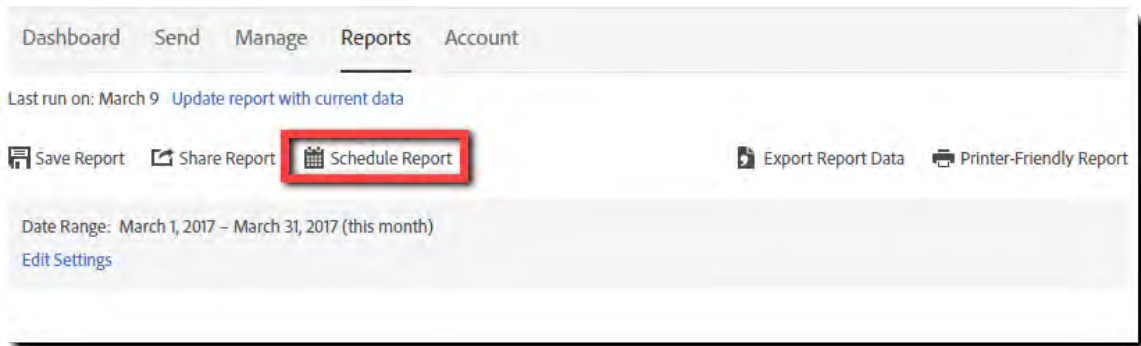
Share Report

Sharing allows you to send the report results to someone else. You just need to enter their email address and a message.



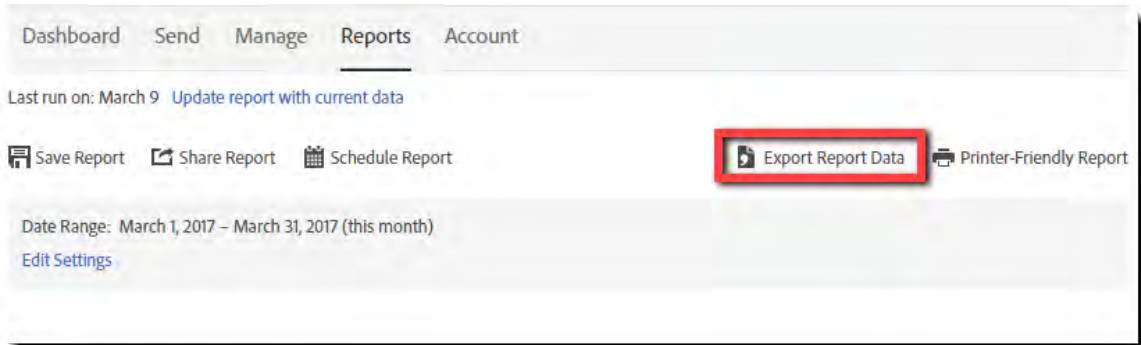
Schedule Report

Setting a schedule for this report will run it with the same parameters at the frequency you define.



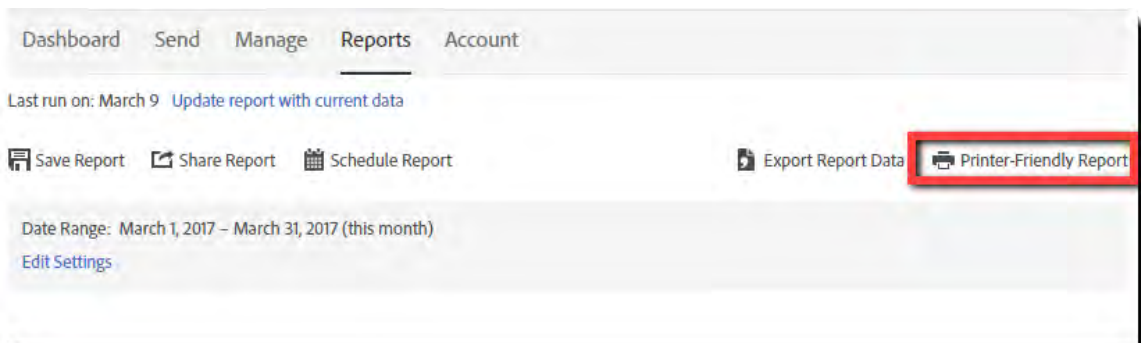
Export Report Data

Clicking this link will prompt you to open or save a .CSV file. CSV files can be opened in Excel and all transaction information for the agreements in the report, will be categorized in the various columns.



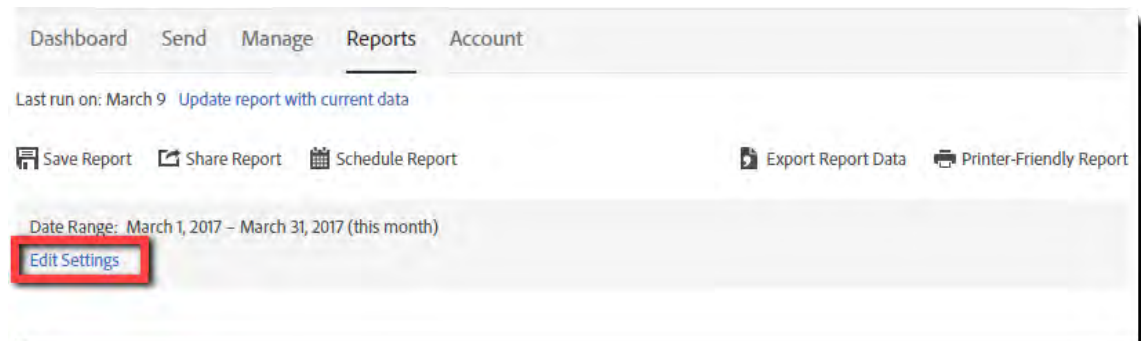
Printer-Friendly Version

Clicking this link will open a printer-friendly version of the report.



Edit Settings

This link will open and permit editing of the configured parameters for the report.






Implementing Adobe Sign

A best practices guide


May 2016

Get a Document Signed

To  kfoyer@globalcorp.com 

Show Cc  signer2@acmeagency.com

☒ I need to sign



Upload

Drag files here

Send Options

☒ Set password to open signed PDF

Signature Types

☒ eSignature ☐ Fax Signature

Send

TABLE OF CONTENTS

3	Transform your business processes with electronic signatures
4	1. Define your objectives and business goals
6	2. Build your implementation team
8	3. Select, prioritize and transform business processes
12	4. Develop your implementation plan
17	5. Implement your project
18	Expand on your success
19	Looking forward
20	Resources

Transform your business processes with **ELECTRONIC SIGNATURES.**

With *Adobe Sign*, an Adobe *Document Cloud* solution, you can automate signing and approvals across a wide range of departments and business processes—helping your organization reduce processing time from days to minutes, deliver great customer experiences, and improve productivity and mobility.

Adobe is committed to the success of your implementation project. As a trusted business partner, we provide the services of both a Customer Success Manager (CSM) and an onboarding specialist to support you throughout your project. In this guide, you will find everything you need for a successful *e-signature* implementation—step-by-step instructions and Adobe best practices, plus additional resources.

Adobe Sign is helping us streamline internal and external processes across the company, making it one of the most value-added products we've ever seen at TiVo.

LARRY DENNY

Vice president and associate general counsel
TiVo

1 Define your objectives and business goals

1a. Define project objectives

Specify what you are trying to achieve, how will you will achieve it and how you will define success for your project. Start by reviewing why your organization is implementing *electronic signatures* (e-signatures):

What needs and challenges did you identify when evaluating e-signature solutions? Examples include:

- Business is slowed or delayed waiting for physical signatures
- High shipping and mailing costs of documents to secure signatures
- Delays in obtaining approvals and signatures due to travel

Where is business delayed due to paper-based, manual processes? Examples include:

- Slow recruiting, hiring and onboarding due to manual process of signing and returning paperwork
- Legal reviews and approvals slowing business
- Nondisclosure agreement (NDA) processes burdened by long review and approval cycles

Where have delays in getting signatures resulted in lost opportunities? Examples include:

- Sales lost or delayed due to challenge of getting signatures
- Longer than desired quote-to-cash process
- Procurement delayed while waiting for required approvals and signatures

Examples of project objectives:

- Reduce the time to process contracts by 75%
- Ensure 24-hour turnaround on reviews and approvals of contracts with mobile e-signing
- Revamp NDA process from Salesforce; require no more than two clicks to generate and send a standardized contract prefilled with accurate data

Best Practice

Not sure where to start?

- Use your Adobe onboarding specialist as a resource to help you define your project objectives.
- Visit [Adobe Sign: Ask Me Anything Webinars](#).

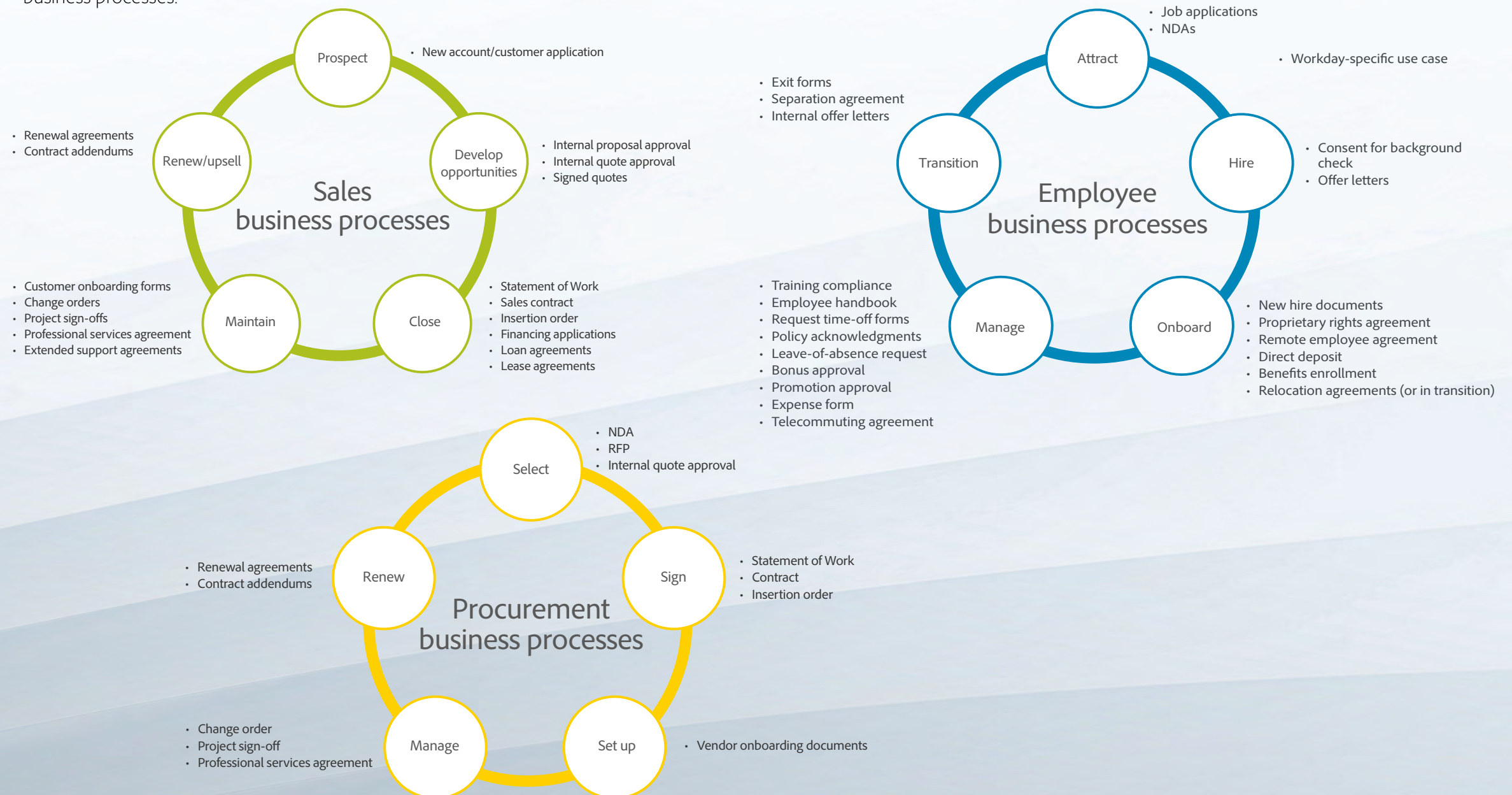
Resources

For more ideas for project objectives and to see how leading organizations are using Adobe Sign, review the business processes in the [Adobe Sign customer showcase](#).

1 Define your objectives and business goals

1b. Review business processes

To get an idea of what business processes can be transformed, review how leading companies are using e-signatures. To see how Adobe is using Adobe Sign to streamline its own internal workflows, read these customer stories: [HR](#), [Legal](#) and [Procurement](#). This diagram shows three common areas where e-signatures are used: sales, employee and procurement business processes.



2 Build your implementation team

Your onboarding specialist will help you select the members of your implementation team—from your organization and Adobe. Depending on the size of your organization, there may be more than one person in each role, one person might hold several roles, or they may overlap.

Customer roles and responsibilities

Customer role	Responsibility	Pairing with Adobe
Executive sponsor (CIO, VP of sales, VP of HR, VP of procurement)	Ultimate point of escalation: <ul style="list-style-type: none">• Drives the vision, directs strategy and gains organization buy-in for the overall project• Attends quarterly business review (QBR) meetings and agrees on next steps• Resources the team, identifies the project manager and ensures success metrics are defined and tracked	Adobe executive sponsor
Line of business manager (VP; director; sr. manager of sales, HR, procurement)	Key stakeholder in defining business objectives: <ul style="list-style-type: none">• Ensures project team has resources and company support needed• Ensures success metrics are defined and tracked	Adobe Customer Success Manager (CSM)
Project manager	<ul style="list-style-type: none">• Works with key stakeholders to define business objectives• Identifies and understands key business processes• Develops implementation plan, and identifies and directs resources needed to deploy integration• Gathers documents needed for rollout• Drives day-to-day management of project including timeline and milestones• Transitions to business as usual at end of implementation	Adobe Customer Success Manager, Adobe onboarding team
Support team	<ul style="list-style-type: none">• Administers Adobe Sign, managing users and settings• Identifies additional e-signature opportunities• Triage any issues and provides answers to internal questions	Adobe Document Cloud support team
Technical implementation manager (if needed)	<ul style="list-style-type: none">• Manages and deploys any API or other integrations or internal work needed to deploy Adobe Sign	Adobe onboarding team, Adobe solutions consulting team
Internal communication manager	<ul style="list-style-type: none">• Communicates with internal stakeholders	Adobe Customer Success Manager

Best Practice

Include owners of these areas on your team:

- Owners of the workflow for the targeted process
- Owners of documents that are targeted for e-signing and approvals
- Document processors involved in postsigning or approval
- Coordinators who interact with parties who will need to sign the documents

2 Build your implementation team

Adobe roles and responsibilities

Adobe role	Responsibility	Pairing with customer
Executive sponsor	Ultimate point of escalation: <ul style="list-style-type: none">• Maintains engagement with customer's executive sponsor• Provides perspective on wider vision and strategy	Customer's executive sponsor
Customer Success Manager	Primary point of contact at Adobe: <ul style="list-style-type: none">• Assesses priorities and goals regarding the use and adoption of Adobe Document Cloud• Provides best practices recommendations and tips to drive adoption• Facilitates introduction of Adobe Solution Partners• Develops success plans• Presents product development road map• Gathers and champions your feature enhancement requests• Demos new releases of Adobe Sign	Customer's project manager and line of business manager
Onboarding specialist	Conduit to any additional resources needed during start-up phase: <ul style="list-style-type: none">• Ensures you have the resources and training to enable the business process transformation• Provides support during initial implementation through configuration and customization of your Adobe Sign account• Holds regular, twice-weekly virtual office hours to answer questions• Connects you to an onboarding email series that provides answers to common onboarding questions, best practices and links to support	Customer's project manager and technical implementation manager
Solutions consulting team and extended services (fee-based services)	<ul style="list-style-type: none">• Adobe Professional Services—Provides solution architects to help you create, develop, deploy, customize or optimize your implementation. Packages and custom services are available in consulting, development and education. For more information, contact your CSM.• Adobe Extended Services—Provides a comprehensive set of proactive support services. For more information, contact your CSM.	Customer's technical implementation manager

Best Practice

Maximize your investment with Adobe services that are included with your subscription. For more information, read the [Adobe Document Cloud Customer Success datasheet](#).

3 Select, prioritize and transform business processes

3a. Select and prioritize business processes

Review your project objectives and targeted lines of business (step 1), and then use them to generate a list of related business processes. If you have already identified the process you want to transform, skip to step 3b, "Transform business processes."

Most processes fall into one of these general categories:

- **Quick win**—A straightforward business process that can be quickly and easily transformed
- **Major opportunity**—Significant organizational reward; good targets for the second phase of your project
- **Special effort**—Deserving of further review to determine implementation complexity and organizational importance
- **Low yield**—Best reexamined after progress in other categories

Once you have a list of business processes, you can prioritize them to determine phasing and targeting. Start with a quick win—an important business process that is easy to implement.

Best Practice

- Start with a quick-win to allow you to work with a small team with focused goals, helping to ensure the first phase of your project can be rolled out quickly—demonstrating success, generating excitement and delivering ROI.
- Identify an important process that is valuable to the business and straightforward to implement. For many companies, NDAs, sales or HR onboarding are a good place to start.

We can complete contracts in minutes and meet deadlines that would have been impossible without leveraging this type of technology.

CONNIE BRENTON

Director of operations and chief of staff, legal department
NetApp

3 Select, prioritize and transform business processes

3b. Transform business processes

The next step is to transform your current business process workflow into a digital workflow. This is a great opportunity to improve your overall process design. Below is an example of how you can dramatically increase the efficiency of your workflow—saving time and resources.



3 Select, prioritize and transform business processes

3b. Transform business processes

1. Document current paper-based workflow

Start by evaluating and then diagramming the current paper process—identifying the documents, actions, stages and delivery mechanisms.

2. Map out your digital process

Using the paper business process workflow diagram, reevaluate the existing process and look for ways to achieve efficiencies.

3. Make documents e-sign ready

Digital documents can simplify the user experience by preventing errors and minimizing re-work. Setting up required fields, format specification, tool tips and data validation are great ways to transform your digital document and improve the user's signing experience. Consider redesigning your documents and forms with selective use of color, layout, reorganization, fonts and data entry fields.

Best Practice

As you document the current workflow, keep track of the time and resources it requires, and where there are issues. You will use these facts later to determine the success criteria for your implementation.

For guidance on transforming workflows, read [Migrating workflows from paper to digital](#).

Resources

- For detailed information on transforming workflows, see the best practices guide [Migrating workflows from paper to digital](#).
- Your Adobe onboarding specialist can help you identify ways to optimize your digital processes.
- For step-by-step instructions on setting up templates that create forms with easy-to-use fillable fields, see this tutorial on [how to create forms with text tags](#).
- For additional examples of the digital transformation of customer workflows, visit the [Adobe Sign customer showcase](#).

3 Select, prioritize and transform business processes

3c. Identify success metrics

You established your project objectives in step 1. It is critical to define the metrics that will be used to determine the success of your project.

- Start with the time and resources that were consumed by the process prior to digital transformation. Which resources were pain points in the process? Which ones are targeted for reduction with e-signatures?
- What are the most important elements of your business processes that owners and participants want to transform? Examples include reducing time or cost to complete, overall percentage of documents transitioned to digital and so on.
- To have the most impact, identify metrics that have the most importance to the targeted audience.

Here are some examples of success metrics:

- Accelerated turnaround time
- Number of signature processes transitioned to digital
- Cost and resources reduction, including shipping and postage costs
- Reduction of quote-to-invoice time by x%
- Reduction of time to onboard new employees or customers by x%

Best Practice

When you documented your paper-based workflow in step 3b, we suggested keeping track of the time and resources it required. Refer to this information as a starting point for your success metrics.

Resources

This tool can help you determine possible success metrics for your organization:

- [Resource Saver Calculator](#)

4 Develop your implementation plan

4a. Implementation strategy

Your implementation plan should specify the phasing, schedule, scope, audiences and/or geographies of the rollout. You will also create plans for communications, training and end-user support.

Integrating with critical business systems

If you are integrating with key business systems such as Salesforce, Workday, Microsoft Dynamics CRM, Microsoft SharePoint or Apttus, you should involve your IT team at this stage.

Once you have identified which business system integrations are in scope, work with your onboarding specialist, CSM and partners to create the detailed plan and timeline for these systems.

Best Practice

If you are integrating to a proprietary business system or want to build a custom application with integration to Adobe Sign, explore using the Adobe Sign API to build a variety of different integrations. For more information, see [Adobe Sign API Guide](#).

Resources

- To find out how to use the Adobe Sign API, see [Adobe Sign API Guide](#).
- To learn more about implementation strategies, read [Creating an Effective Deployment Strategy for Adobe Sign](#).
- To learn about implementation strategies of leading companies, review [customer success stories](#) and Adobe success stories: [HR](#), [Legal](#) and [Procurement](#).
- View the [list of business system integrations](#) Adobe Sign supports today. For more information, consult the [Adobe partner integration guides](#).

4 Develop your implementation plan

4b. Communication plan

The goal of the communication plan is to generate excitement about the move to e-signatures and to ensure everyone in the organization knows how it will affect their workflows.

Identify target audiences

Begin by identifying the target audiences you need to communicate with and the most effective communication channel for each audience.

Communication channel recommendations for typical audiences

Internal

Executives	<ul style="list-style-type: none">• Face-to-face presentation• Email
Legal	<ul style="list-style-type: none">• Face-to-face presentation• Follow-up reference guide
Users	<ul style="list-style-type: none">• Training webinar• Email• Intranet documentation• Weekly drop-in call• Lunch and learn• Internal social media: Chatter, Yammer and so on
Signers/customers	<ul style="list-style-type: none">• Newsletter email• FAQ page on website• Social media posts
Partners/subsidiaries	<ul style="list-style-type: none">• Training webinar• Email• Weekly drop-in call• Lunch and learn
Banks*	<ul style="list-style-type: none">• Face-to-face meeting• Official communications to go paperless

* If using Adobe Sign for automatic payment authorizations or direct debit mandates (UK)

Best Practice

- Follow the recommendations in [Creating an effective deployment communication plan](#).
- Create an elevator pitch about why your organization is moving to e-signatures. Concisely explain the project, identifying the benefits and explaining the risks and costs of maintaining manual signature processes. This pitch can be reused in almost all communications.

Resources

- For more details on developing content, read the best practice guide [Creating an effective deployment communication plan](#).
- For more information on e-signatures, visit the [Adobe Sign website](#) and [Adobe Sign FAQ](#).

4 Develop your implementation plan

4c. Training plan

Your training materials should provide users with a clear understanding of the overall changes to the business process, as well as how and why the new workflows will help speed your implementation project.

1. Train your program team

Your onboarding specialist offers joint training sessions for administrators and end users to get you started.

2. Identify additional audiences to train

Next, you will identify the audiences you need to train and determine the training resources these audiences will require.

3. Provide a variety of training resources

Help ensure that users can find help at any point during the project by providing a variety of training resources. FAQ, checklists and peer-to-peer sharing are great ways to preserve and reuse knowledge

Get questions answered by your Adobe onboarding specialist

Your onboarding specialist hosts twice-weekly [Adobe Sign: Ask Me Anything Webinars](#). Designed for you to ask questions, seek advice or get recommendations, you can drop in anytime to these open, virtual office hours.

Enhance your team's expertise with Adobe Professional Services

Adobe provides expert services designed to help you develop your team's skills and gain greater control of your implementation project. Educational resources are also available.

Best Practice

- Follow the guidelines in [5 steps to developing an effective training plan](#).
- Your Adobe onboarding specialists and CSMs can train a "super user" from your organization, and then this individual will train your internal users. This can help speed resolution to internal questions during implementation.

Resources

- [On-demand training videos](#)
- [Adobe Sign online help](#)
- [Adobe Sign reference guides](#)
- [Best practice articles](#)
- [5 steps to developing an effective training plan](#)
- [Adobe Sign: Ask Me Anything Webinars](#)
- Quarterly best practice-focused webinars via email invitation

4 Develop your implementation plan

4d. Support plan for end user

The goal of the support plan is to provide timely responses to any issues or questions that may arise to ease the transition to the new technology. Include a broad range of self-service tools, as well as in-person support to handle different types of questions.

Adobe support

With Adobe Sign, you get how-to support designed to answer your critical questions via web, email, live chat and phone. Adobe Document Cloud provides industry-leading availability and support response times.

When you need additional support day or night, you can visit and participate in the [Adobe Sign community forums](#):

- Access blogs
- Read FAQ
- Submit feature requests
- Connect with other customers to share best practices and lessons learned

Additional support options

Paid service offerings enhance and extend the support you already receive as an Adobe Sign customer. Our Extended Service for Adobe Sign customers provides a more hands-on, personalized relationship with Adobe for expertise in a complex environment and assistance for a multifaceted solution. For more information, contact your Adobe CSM.

Best Practice

- To get answers to less urgent, but important questions during your implementation project, attend one of the twice-weekly [Adobe Sign: Ask Me Anything Webinars](#) offered by your onboarding specialist.

Resources

- Reach support specialists by signing into your account from the support page. Once you have signed in, you can submit a support ticket or connect with technical support specialists 24x7 via live chat. You can also reach a support specialist by phone.
- Join a user group to share information, ask questions and get to know other users. Contact adobesignusergroups@adobe.com to sign up today.

4 Develop your implementation plan

4e. Integrated implementation plan: Putting it all together

Once your implementation approach, training, communication and support plans are in place, you will want to combine them into one comprehensive rollout plan. This integrated program schedule should include regular check-in meetings, milestones and metric measurements.

Best Practice

Assess and identify risks that may impact your implementation. Key risk management steps are:

- **Identify risks**—Brainstorm all potential project risks.
- **Assess risks**—Prioritize risks based on impact.
- **Develop a risk response**—Identify ways to manage or prevent the risk.
- **Develop a contingency plan or preventative measures**—Convert risk response into tasks.

With Adobe Sign, we can see where our contracts are at all times. The added visibility strengthens client relationships and frees up time for us to focus on other critical activities.

JOOST VAN DE BUNT
Business development manager
KLM

5 Implement your project

Hold regular status meetings

During your implementation, hold regular status meetings to track detailed plan execution, measure progress and execute course corrections, if needed.

Measure and report success

Regular measurement and reporting on your success metrics will help ensure you can readily identify successes, as well as any areas that need improvement.

Review project risks and mitigation plans

Regularly review risks and mitigation plans, and track your results and metrics. Should any risks increase in likelihood, discuss them at your regular status meeting to develop a risk response.

Quarterly business reviews

Your Adobe CSM will schedule joint quarterly business reviews (QBRs). These reviews are a significant opportunity to get visibility into any project in progress, as well as expand the focus to other areas where e-signatures can be utilized in your organization. QBRs are most effective when your executives are involved.

Best Practice

Use this best practice agenda for your QBR. Make sure your full account team attends the meeting.

- Utilization statistics
- Support tickets
- Current and future implementation review
- Recommendations
- Adobe roadmap
- Important dates and next steps

Adobe Sign makes the contract process seamless. We can update templates centrally and maintain control over our client and sales communications, confident that all contracts adhere to legal requirements.

JAY KLAUMINZER

Head of North American local business
Groupon

Expand on your success

Measure progress and share success

1. Regularly measure and record progress

Use the success metrics defined at the beginning of the project to ensure you have solid data detailing the benefits of the transformation. Regularly measure and record progress against these metrics.

2. Determine lessons learned

Gather input from users and stakeholders on the lessons learned from the project.

- What went well and contributed to the success of the program?
- What unanticipated benefits were derived?
- What risks occurred that weren't anticipated?
- Are there any additional areas that could have been improved during the project?

3. Celebrate success

Share your success with e-signatures with other groups and departments using the [Adobe Sign Share Your Success kit](#). Gather feedback to identify other areas that could benefit from e-signatures.

4. Identify the next phase of your implementation project

Review your prioritization list and the business processes on page 5 to decide the next phase of your implementation project. Remember that any process that requires a physical or wet signature is an opportunity for e-signing.

Best Practice

- Use the [Adobe Sign Share Your Success kit](#) to celebrate your success and demonstrate the benefits of e-signatures to key stakeholders in your organization.

Resources

- Use the [Adobe Sign Share Your Success kit](#) to share the benefits of e-signatures with key stakeholders in your organization.

Looking forward

Build on your momentum

Continue to build your rollout plan to help ensure continued adoption and success of e-signatures at your organization.

As you roll out e-signatures throughout your company, build on your success by creating an e-signature infrastructure:

- **Create an e-signature system architecture**—Create a system architecture that consolidates all lines of business, business processes and geographies, and critical systems your organization integrates with.
- **Create an Adobe Sign center of excellence**—Track the success and use of e-signatures in your organization. When new lines of business are considering e-signatures, provide advice and assistance to help them make the move.
- **Create an effective e-signature policy**—Your legal department can create a master signature policy to help guide your organization's efforts.
- **Define a data retention policy**—Your legal department can examine and define your organization's data retention policy. Adobe Sign supports a customizable data retention policy that can be configured to delete documents and collected data from Adobe Sign. It complies with several industry standards for data security and availability such as PCI DSS 3.0, HIPAA, SOC 2 Type II and ISO 27001.

Best Practice

Use this guide as a reference for your next project.

Resources

- [Developing an effective electronic signature policy](#)
- [Adobe Sign Document Retention](#)

Resources

1. Define your objectives and business goals

- How leading companies are using Adobe Sign
 - [Adobe Sign customer showcase](#)
- How Adobe uses Adobe Sign
 - [HR](#)
 - [Legal](#)
 - [Procurement](#)

2. Build your implementation team

- Customer success services will help you get started
 - [Adobe Document Cloud Customer Success datasheet](#)

3. Select, prioritize and transform business processes

- Best practice: Workflows
 - [Migrating workflows from paper to digital](#)
- Best practice: Templates
 - [How to create forms with text tags](#)
- Best practice: Integration
 - [Adobe partner integration reference guides](#)
- Success metrics tool
 - [Resource Saver Calculator](#)

4. Develop your implementation plan

- Learning about e-signatures
 - [Adobe Sign website](#)
 - [Adobe Sign FAQ](#)

- Adobe Sign API
 - [Adobe Sign API Guide](#)
- Best practice: Implementation strategies
 - [Creating an Effective Deployment Strategy for Adobe Sign](#)
- Implementation strategies of leading companies
 - [Customer success stories](#)
 - Adobe success stories: [HR](#), [Legal](#) and [Procurement](#)
- System integrations with Adobe Sign
 - [List of the business system integrations](#)
 - [Adobe partner integration reference guides](#)
- Best practice: Developing a communication plan
 - [Creating an effective deployment communication plan](#)
- Developing a training plan
 - [On-demand training videos](#)
 - [Adobe Sign online help](#)
 - [Adobe Sign reference guides](#)
 - [Best practice articles](#)
 - [5 steps to developing an effective training plan](#)
 - [Adobe Sign: Ask Me Anything Webinars](#)
 - [Adobe Sign Share Your Success kit](#)
 - Quarterly best practice-focused webinars via email invitation

Expand on your success

- Best practice: Sharing the benefits of e-signatures throughout your organization
 - [Adobe Sign Share Your Success kit](#)

Looking forward

- Best practice: Creating an e-signature policy
 - [Developing an effective electronic signature policy](#)
- Best practice: Defining a data retention policy
 - [Adobe Sign Document Retention](#)





Sign In



SIGN ▾

Adobe Sign User Guide

Search Adobe Support



Search

Welcome to Adobe Sign!

Before you begin using Adobe Sign, we've got some basics to run through. The purpose of this guide is to get you familiar with Adobe Sign and the functionality available to you as a user.

This guide covers all the important processes in Adobe Sign and familiarizes you with the user interface. The Adobe Sign Help system provides more in depth information where needed. If you are connected to the Internet, you can click on the links in the grey boxes that begin with the text "Additional information ..." to view the related help topics.

Note:

Where applicable, features and functions specific to *Adobe Sign – Business*, *Adobe Sign – Enterprise*, or both are noted. This guide documents the features and functions available at the highest level of license agreement, *Adobe Sign – Enterprise*. To determine your license type, go to *My Profile*. If you have questions about the features available for your license, please contact your Client Success Manager or [Adobe Sign Support](#).

Adobe Sign is a highly customizable application with a wide range of features that may or may not apply to how you do business. Your account administrator or group administrator may have disabled some of the options described. If you have a need for something you don't see available to you, contact your group or account administrator. Our service supports different configurations for different groups so even if it's best to have a feature disabled for one group, it's possible to have it enabled for another.

By the end of this guide, you'll be familiar with all of the standard "send" workflows in Adobe Sign as well as how to manage your agreements, and how to generate reports so you can stay on top of what's complete, and what is still pending.

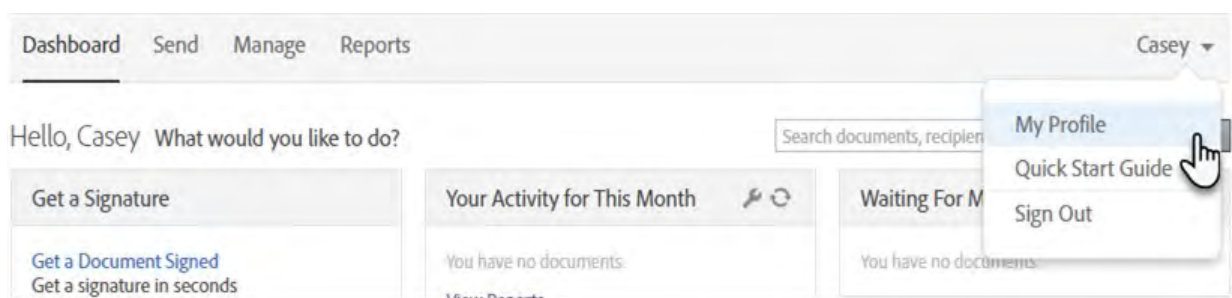
Personalize your Account

When you first log into Adobe Sign, take a minute to review your personal user information. This information is used in several templates, so it's important to ensure it is correct.

- Mouse over your name in the upper-right corner to open the menu, and click **My Profile**

ON THIS PAGE

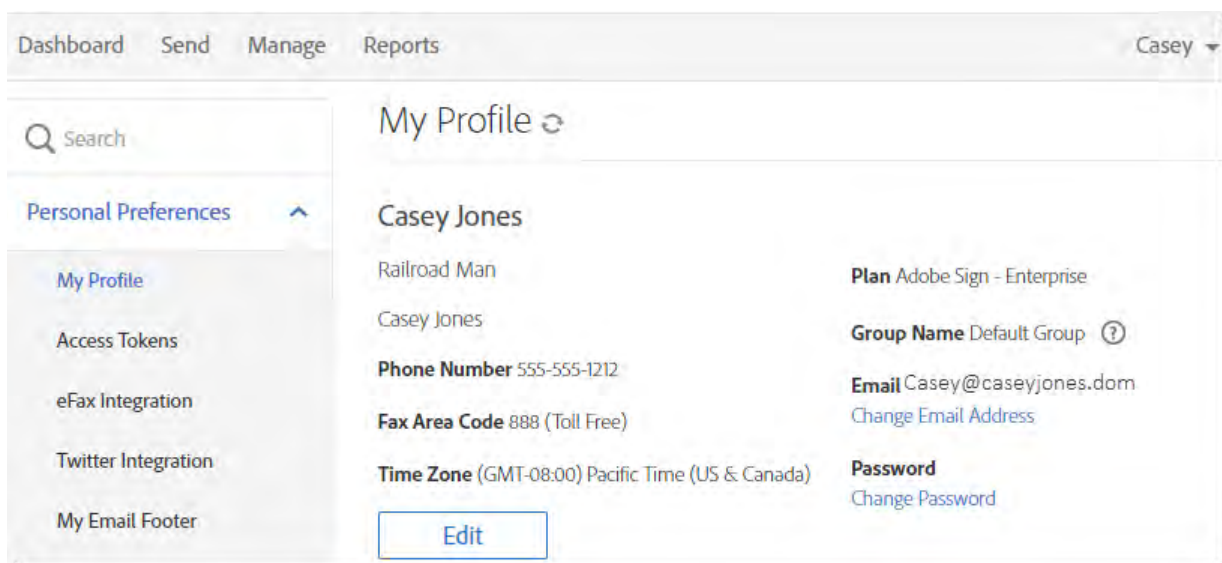
[Welcome to Adobe Sign!](#)[Page by Page Overview](#)[Sending Agreements](#)[Signing Environment](#)[Managing Agreements](#)[Reports \(Adobe Sign – Business and Enterprise\)](#)[Preview and Authoring Experience](#)[Library Templates](#)[Alternate Workflows for Signatures](#)[Mobile Devices](#)Applies to: **Sign**Last Published: **September 21, 2017**



The profile page shows the specific values that Adobe Sign will use when personalizing any of your transactions. Of particular interest are:

- Your full name – Used in email communications and for your default typeset signature
- Your job title – Automatically populates if you ever have a Title field to fill in
- Your company name – Reflected in email communications, this should be the full legal company name
- Time Zone - Time/Date stamps will be cast in your time zone for better clarity when running reports.

If you need to adjust any of the content, click the **Edit** button, make the required changes, and then **Save** your edits.



After configuring your personal information, take a quick look through the other personal preferences you see listed on the left side of the screen. These options are specific to you as a user, and may be useful automations:

- **My Profile** – Your personal identifying information

- **Access Tokens** – If you are a developer, this is where your API tokens are defined and listed
- **Twitter Integration** – Send a Tweet every time an agreement is completed!
- **My Email Footer** – Add a custom (plain text) footer to the bottom of your email templates when sending new agreements
- **Auto Delegation** – Automatically delegate any Adobe Sign agreements sent to you for signature to the named party. Similar to an “Out of Office” forwarding process for Adobe Sign agreements
- **My Events/Alerts** – Configure which types of events/alerts you want Adobe Sign to notify you about, and how you want to be notified. You can get real time email, or log the event and set up reporting on a daily or weekly cycle. (Events are triggers when something happens. Alerts are triggered when a time interval passes and something doesn’t happen)
- **Shared Events/Alerts** – If another user’s account is shared with you, you can customize which of their events and alerts you’d like to be informed of
- **My Signature** – Upload an image of your signature and initials. PNG files work best
- **Language Preferences** – There are two settings to consider under this heading:
 - **My Language Preference** – This setting allows you to define the language used for you within the Adobe Sign web application.
 - **Signing Language** – This setting defines the default language used for the email notifications and the recipient’s guided signing experience.
- **View Other Accounts** – If you need to view the agreements on another user’s account, you can request that here. A list of all viewed accounts will be enumerated. This is a “read only” perspective
- **Share My Account** – If you need to share your account to another person, you can specify who can see your agreements here. Sharing your account is a view only. The viewer cannot sign, cancel or delegate

Page by Page Overview

- **Dashboard Page**
- **Send Page**
- **Manage Page**
- **Reports Page**

Sending Agreements

Sending documents and collecting signatures and approvals is what Adobe Sign is all about! Every customer has different requirements regarding who needs to

interact with the document and in what order, so there are a number of workflow features available in the Send page interface you should know about.

Dashboard Send Manage Reports Account Casey ▾

What's New!

Recipients

Complete in Order ☒ Complete in Any Order ☐ Add Me Add Recipient Group ?

1	fclark@gmail.com	Email		
2	severtonea@gmail.com	Email		
3	rsmithers@gmail.com	Email		
4	jmartin@gmail.com	Email		
5	Enter recipient email			

Show CC

Message

Agreement Name

Please review and complete this document.

Options ?

☐ Password Protect

☐ Completion Deadline

☐ Set Reminder

Recipients' Language

English: US ▾

Files Add Files

Drag & Drop Files Here

☐ Preview & Add Signature Fields

Send

- Recipients Section
- Hybrid Workflows
- Recipient Groups
- Message Section
- Options Section
- Files Section

➤ **Sending an Agreement to One Recipient**

Signing Environment

Experiencing the signing process is helpful in understanding the end result of the configurations done by the sender.

➤ **The Signers Experience**

Managing Agreements

Managing your agreements is an important part of working with Adobe Sign. Use the Manage page to track, process, and customize agreements. Whether it's canceling an agreement or replacing the signer, these processes allow you to influence the transaction's progress in the system.

➤ **Manage Page Structure**

➤ **Agreement Tools**

➤ **Quick links to common tasks**

Reports (Adobe Sign – Business and Enterprise)

The report feature lets you check on how your account is using Adobe Sign. Build your own reports and gain complete visibility into your document signing process, while seeing how individual groups or users are doing.



➤ Creating Reports

➤ Report Results

Preview and Authoring Experience

The Authoring environment provides the form building functionality for Adobe Sign. Beyond placing signature fields, you can include fields that auto-populate content, like the date or the signers signature values (when known), or text fields that do content validation and/or complex calculations. Other common field types such as dropdown boxes, radio buttons and check boxes are also available

➤ Accessing the Authoring Environment

➤ Authoring Environment

Library Templates

A library template is a reusable object. Adobe Sign supports two types of library templates: document templates and form field templates.

- **Document Templates**—A document template is a reusable document. Document templates can be shared with other users in your account, allowing multiple users to send out the same document without needing to make any changes.

- **Form Field Templates**—A form field template is a reusable field layer that can be applied to any document. Form field templates can also be shared with other users in your account. Form field templates are ideal in the following situations:
 - You have one field layout that works for multiple documents.
 - You have a document that can be sent a number of different ways.
 - You need to revise document's content, but the fields remain in the same place.

Instead of creating a new library document every time a document is updated, the same form field layer can be applied. Form field templates can be edited to facilitate changes in the arrangement of fields or field properties. Again, all the tools in the authoring environment are available when creating a form field template.

As a best practice, a single user (Document Administrator) should be responsible for creating and maintaining templates. Creating a Doc Admin user login eliminates confusion as to what templates to use and provides version control for your reusable documents.

We recommend using a distribution list or functional email for the Doc Admin user login. This allows you to control access to this Doc Admin login while at the same time allowing the responsibility to be shared as needed.

Additional information on using the authoring tools to create templates can be found in the Adobe Sign Help by clicking [here](#).

➤ Creating a Library Template

➤ Using a Library Template

Alternate Workflows for Signatures

There are a number of workflows you can use to send documents for signatures, collect signatures, and send a signed document including the following:

- Sending Using "Only I Sign"
- Sending Using Mega Sign (Adobe Sign – Business and Adobe Sign – Enterprise)
- Using Widgets to Collect Signatures (Adobe Sign – Business and Adobe Sign – Enterprise)

The following sections discuss each of these processes in more detail.

Additional information on sending agreements can be found in the Adobe Sign Help by clicking [here](#).

➤ Sending to Multiple Recipients

➤ Only I Sign

- [Mega Sign \(Adobe Sign – Business and Enterprise\)](#)
- [Widgets \(Adobe Sign – Business and Enterprise\)](#)

Mobile Devices


Signing is one the main functions of Adobe Sign. Anyone can sign via an email link on any web browser on their computer or using their mobile device. If you have an Adobe Sign account, you can also sign using the “Adobe Sign manager” iOS or Android native app. You can also initiate signing from the Manage page. Signing is also built into the “Only I Sign” process.

Additional information on signing documents using an app can be found in the Adobe Sign Help by clicking [here](#).

Adobe Sign supports the latest web browsers on smartphones and tablets that run the iOS or Android operating systems.

- [Adobe Sign Manager for iOS](#)
- [Adobe Sign Manager for Android](#)

DOWNLOAD

 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

[^ Back to top](#)

Ask the Community

Post questions and get answers from experts.

[Ask now](#)

Contact Us

Real help from real people.

[Start now](#)

[Sign In](#)**SIGN** ▾

System requirements for Adobe Sign

System requirements

Search Adobe Support

ON THIS PAGE



The following system requirements apply to Adobe Sign (formerly Adobe Document Cloud eSign services or Adobe EchoSign).

Browser

- Microsoft Windows 10 using Microsoft Edge, Internet Explorer 11, Firefox, or Chrome
- Microsoft Windows 8 using Internet Explorer 11 or later, Firefox, or Chrome
- Mac OS X v10.9 or later using Safari 7 or later, Firefox, or Chrome

Note:

The Microsoft Edge browser does not natively support 256-bit AES encryption of PDF files.

If you are using the Edge browser, please ensure you are running the latest version of [Adobe Reader](#)

[System requirements](#)

[Language versions](#)

[Supported document formats for signature](#)

[Application/Protocol Requirements](#)

[Software required to view a signed document](#)

[IP Ranges to Whitelist](#)

[SSL Certificate Authority / Certificates \(Active as of May 2, 2018\)](#)

Applies to: **Sign**

Last Published: **May 7, 2018**

Mobile app

- Adobe Sign: [iOS](#), [Android](#)

Language versions

US English	Japanese	Croatian	Danish
UK English	Chinese	Czech	Dutch
French	(Simplified)	Polish	Finnish
German	Chinese	Romanian	Hungarian
Spanish	(Traditional)	Russian	Icelandic
Catalan	Korean	Slovenian	Italian
Basque	Indonesian	Slovakian	Norwegian
Brazilian	Malay	Turkish	Swedish
Portuguese	Thai	Ukrainian	
Portuguese	Vietnamese		

Supported document formats for signature

- Adobe PDF (.pdf)
- Microsoft Word (.doc and .docx)
- Microsoft Excel (.xls and .xlsx)
- Microsoft PowerPoint (.ppt and .pptx)
- Text (.txt)
- Rich Text (.rtf)
- Graphics (.tif, .jpg, .jpeg, .gif, .bmp, and .png)
- Web (.htm or .html)

Application/Protocol Requirements

➤ Java Requirement

➤ TLS 1.2 Requirement

Software required to view a signed document

- Adobe Reader 9.0 or later for documents secured with AES 128-bit encryption or lower
- Adobe Reader 10 or later for documents secured with AES 256-bit encryption

Adobe online services are available only to users 13 and older and require agreement to additional terms and the [Adobe Privacy Policy](#). Online services are not available in all countries or languages, may require user registration, and may be discontinued or modified in whole or in part without notice. Additional fees or subscription charges may apply.

IP Ranges to Whitelist

If you explicitly whitelist IP addresses on your network, please add the below IP ranges to your firewall:

North America:

- 52.71.63.224/27
- 52.35.253.64/27
- 40.67.155.147/32
- 40.67.154.249/32
- 40.67.155.185/32
- 40.67.155.112/32

Europe:

- 52.48.127.160/27
- 52.58.63.192/27

Japan:

- 52.196.191.224/27

Australia:

- 52.65.255.192/27

India:

- 13.126.23.0/27

IP ranges for outbound mail relays

If your organization whitelists IP addresses to control connection to your inbound mail servers, add the following IP addresses to your whitelist:

- 40.67.157.141/32
- 40.67.154.24/32
- 40.67.158.131/32
- 52.205.63.172/30
- 52.41.255.236/30
- 52.208.255.252/30
- 52.59.244.0/30
- 52.197.127.252/30
- 52.65.63.248/30
- 13.126.23.32/30

SSL Certificate Authority / Certificates (Active as of May 2, 2018)

Adobe Sign is moving to a new SSL Certificate on May 2, 2018. There is no change to the public key, underlying cryptographic protocols or scheme.

Only the *Adobe Sign Certificate* (listed below) is changing. The *Public Key*, *Root CA*, and *Intermediate CA* will remain the same.

Please contact Customer Support with questions.

DOWNLOAD


[Get file](#) Adobe Sign Public Key

[Get file](#) Adobe Sign Certificate

DOWNLOAD

[Get file](#) Root CA Certificate

[Get file](#) Intermediate CA Certificate

 Twitter™ and Facebook posts are not covered under the terms of Creative Commons.

[Legal Notices](#) | [Online Privacy Policy](#)



SIGN

[^ Back to top](#)

[< See all apps](#)

[Learn & Support](#)

[Get Started](#)

[User Guide](#)

[Tutorials](#)

ADOBE USER GROUP DIRECTORY ▾

[Virtual](#) | [North America](#) | [Latin America](#) | [South America](#) | [Asia Pacific](#) | [Europe, Middle East and Africa](#)

Virtual

[Photoshop and Lightroom \(English\)](#)















[Photoshop Group \(English\)](#)

North America








Canada













Montreal	Communauté Adobe de Montréal
Québec	Communauté Adobe de Québec
Toronto	After Effects Toronto
Toronto	Toronto InDesign User Group





























Canada		ADOBE USER GROUP DIRECTORY ▾			
	Vancouver, BC	Vancouver Adobe InDesign User Group			
Mexico					
	Cancun	Grupo Creativo Mexico			
United States					
Alabama	Auburn	Auburn Multimedia User Group			
Arizona	Phoenix	Phoenix InDesign User Group			
	Phoenix	Phoenix Adobe User Group			
	Tucson	Tucson Adobe User Group			
California	Anaheim	Adobe After Effects Abuser Group			
	Anaheim	Web - Video Crossroads			
	Eureka	Eureka Photoshop User Group			
	Hollywood	Los Angeles Creative Pro User Group			
	Huntington Beach	Adobe Technology Exchange of			












Southern
California
ADOBE USER GROUP DIRECTORY ▾















Los Angeles	Adobe Illustrator User Group LA (AILA)		
Los Angeles	Digital Media Artists Los Angeles (DMALA)		
Los Angeles	The Los Angeles Photoshop User Group		
Los Angeles	LA Web Professionals Group		
Los Angeles	LA Digital Imaging Group (LADIG)		
Los Angeles	Adobe for Fashion Los Angeles		
Los Angeles	Los Angeles InDesign User Group		
Orange	Orange County Adobe Photoshop User Group		
Riverside	Independent Filmmakers of the Inland Empire		
San Diego	San Diego Photoshop Users Group		



	San Diego	San Diego Adobe User Group		
		ADOBE USER GROUP DIRECTORY ▾		
	San Diego	San Diego InDesign User Group		
	San Francisco	Bay Area ColdFusion Users Group		
	San Francisco	Creative Cloud Lovers		
	San Francisco	SF Bay Area Illustrator User Group (ILUG)		
	San Francisco	SF Cutters		
Colorado	Boulder	Boulder Valley Adobe User Group		
	Fort Collins	NoCo Pro Photo		
Connecticut	Hartford	Hartford Adobe User Group		
District of Columbia	Washington	District Digital Creatives - an Adobe User Group		
	Washington	DC MD VA Creative Pro User Group (DMV CPUG)		
	Washington	DC Media Makers		
Florida	DeLand	Tech Deland		











	Jacksonville	ADOBE USER GROUP DIRECTORY 		
		South Florida ColdFusion Users Group		
	Orlando	Orlando Adobe User Group		
	Tampa	Tampa Adobe User Group		
	Tampa Bay	Tampa Bay Creative Suite User Group		
	Tampa Bay Area	Lightroom Tampa Bay		
Georgia	Atlanta	Atlanta Cutters		
	Atlanta	Atlanta InDesign User Group		
Illinois	Chicago	Chicago Adobe Users Group		
	Chicago	Chicago Photoshop User Group		
	Chicago	Chicago InDesign User Group		
	Downers Grove	Chicagoland ColdFusion User Group		
Indiana	Evansville	Evansville Design Group		
	Indianapolis	PodcastIndy		
	Indianapolis	IndyAdobe		

	Indianapolis	Indianapolis ADOBE USER GROUP DIRECTORY 		
		Community		
	Indianapolis	Indy MeetUp Photo Club (IMUPC)		
Kansas	Kansas City	Digital Photography Adobe Community		
	Overland Park	KCVideoCore		
	Topeka	Topeka Camera Club		
Maine	Portland	The Portland Camera Club		
Maryland	Baltimore	Baltimore Adobe Video User Group		
Massachusetts	Boston	Boston Adobe User Group (ABUG)		
	Boston	Boston Creative Pro User Group		
	Boston	United States InDesign User Group Boston		
	Cambridge	Boston Premiere Pro User Group		
Michigan	Detroit	Adobe User Group-Detroit		
	East Lansing			

ADOBE USER GROUP DIRECTORY			
		Mid-Michigan InDesign User Group	
Minnesota	Lakeville	Twin Cities ColdFusion User Group	
	Minneapolis	Twin Cities InDesign User Group	
	Minneapolis	Minnesota After Effects User Group	 
	Minneapolis	Twin Cities Photoshop & Lightroom User Group	
	St. Cloud	Central Minnesota Photoshop User Group	
Missouri	Kansas City	KC-UX-Core	
	Kansas City	KC DesignCore	 
Montana	Bozeman	Bozeman Photoshop Users Group	 
Nebraska	Omaha	Nebraska ColdFusion Users Group	
Nevada	Las Vegas	The Las Vegas Adobe User Group	
New Hampshire	Durham	NH Adobe User Group	

	Nashua	Nashua Adobe User Group		
		ADOBE USER GROUP DIRECTORY ▾		
New Jersey	Union	InDesign User Group of New Jersey		
New Mexico	Virtual	motion+connect		
New York	Clinton	ColdFusion User Group of Central New York		
	New York	New York City InDesign User Group		
North Carolina	Raleigh	Raleigh InDesign User Group		
	Charlotte	Charlotte Animation Visual Effects & Motion Design (CAVEMODE)		
	Charlotte	Charlotte Cutters		
Ohio	Cleveland	Cleveland Adobe Users		
Oregon	Eugene	Eugene InDesign User Group		
	Portland	Ps-PDX		
	Portland	AEPDX - Portland After Effects User Group		
Pennsylvania	Harrisburg			

ADOBE USER GROUP DIRECTORY			Facebook	Twitter
State	City	Group Name		
		Central Penn Group (CPAUG)		
South Carolina	Clemson	South Carolina - Adobe User Group		
	Columbia	Refresh Columbia		
South Dakota	Sioux Falls	SoDak After Effects Group		
Tennessee	Johnson City	VFX & Motion Adobe After Effects User Group		
	Nashville	Nashville Adobe User Group		
	Nashville	Nashville ColdFusion User Group		
Texas	Austin	Austin Adobe User Group		
	Austin	Create ATX		
	Dallas	The Dallas After Effects User Group		
	Dallas	DFW Photography and Adobe Photoshop User Group		
	Frisco	Dallas Premiere Pro User Group		
	Houston	Houston CSS Meetup Group		

	Houston	Houston Adobe User Group		
		ADOBE USER GROUP DIRECTORY ▾		
	San Antonio	Alamo Area Multimedia Users Group		
	San Antonio	San Antonio Web Spinners		
	Spring	The Houston Photoshop Group		
Utah	Salt Lake City	Salt Lake Frontend User Group		
	South Jordan	Digital Photography and Compositing with Photoshop		
Washington	Seattle	After Effects Seattle		
	Seattle	Seattle Adobe Premiere users Group (and related software)		
	Seattle	Seattle Area Photoshop Users Group		
	Seattle	Seattle ColdFusion User Group		
Wisconsin	Madison	Madison Adobe User Group		
	Milwaukee			

Milwaukee
ADOBE USER GROUP DIRECTORY ▾
Group/Graphic
Design Meetup
Milwaukee
Milwaukee
InDesign User
Group

Latin America

Colombia Bogotá Adobe User Group
Latinoamerica



South America

Argentina Buenos Aires Adobe Grupo Usuarios
Argentina



Brazil São Paulo InDesign Brasil

Asia Pacific

Australia Adelaide Adobe User Group –
South Australia (AUGSA)












Brisbane Brisbane InDesign User
Group



	Sydney	Adobe User Group Sydney	
Philippines	Santa Rosa	Graphikarista Adobe User Group	

Europe, Middle & Africa

Armenia	Yerevan	Adobe User Group in Armenia	
France	Paris	InDesign User Group Paris	 
	Paris	All Creative in Paris	
Greece	Athens	Athens InDesign User Group	
Italy	Milan	Illustrator User Group Italia	
	Naples	Adobe Web Design User Group Italia	
	Reggio Emilia	InDesign User Group ITALIA	
	Rome	After Effects User Group Italia	
Kenya	Nairobi		

ADOBE USER GROUP DIRECTORY ▾				
		InDesign User Group Nairobi		
Netherlands	Amsterdam	Adobe User Group Netherlands		
Nigeria		Adobe After Effects Nigeria (AENG)		
Portugal	Lisboa	InDesign User Group Lisboa		
	Oporto	Oporto InDesign User Group		
South Africa	Port Elizabeth	Port Elizabeth Adobe User Group		
Spain	Madrid	InDesign User Group Madrid		
		PhoneGap Spain		
	Palma de Mayorca	Conecta Tutoriales		
Switzerland	Zurich & Bern	InDesign User Group ZH/BE		
United Kingdom	London	London CFML & Web Community		

Appendix A: ITS-400335 Entire Solicitation

Attachment A: Department of Information Technology Terms and Conditions

Attachment B: Enterprise Security & Risk Management Office (ESRMO) Vendor Assessment Guide

STATE OF NORTH CAROLINA Department of Information Technology	REQUEST FOR PROPOSAL NO. ITS-400335	
	Offers will be publicly opened: July 12, 2018	
	Issue Date: June 11, 2018	
Refer <u>ALL</u> inquiries regarding this RFP to: Kristen Burnette kristen.burnette@nc.gov 919-754-6678	Commodity Number: 208	
	Description: Enterprise Electronic Forms and Digital Signature Capability	
	Using Agency: Multiple State Agencies	
See page 2 for mailing instructions.	Requisition No.: NA	

OFFER AND ACCEPTANCE: The State seeks offers for the Online Services and/or goods described in this solicitation. All offers and responses received shall be treated as offers to contract. The State's acceptance of any offer must be demonstrated by execution of the acceptance found below, and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's offer.

EXECUTION: In compliance with this Request for Proposal, and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein. By executing this offer, I certify that this offer is submitted competitively and without collusion.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR:		
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY, STATE & ZIP:	TELEPHONE NUMBER:	TOLL FREE TEL. NO
PRINT NAME & TITLE OF PERSON SIGNING:	FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:

Offer valid for ninety (90) days from date of offer opening unless otherwise stated here: ____ days.

ACCEPTANCE OF OFFER: If any or all parts of this offer are accepted, an authorized representative of AGENCY shall affix their signature hereto and this document and the documents identified above shall then constitute the written agreement between the parties. A copy of this acceptance will be forwarded to the awarded Vendor(s).

<u>FOR AGENCY USE ONLY</u> Offer accepted and contract awarded _____, as indicated on attached certification, by _____ (Authorized representative of DEPARTMENT OF INFORMATION TECHNOLOGY).
--

DELIVERY INSTRUCTIONS: The Vendor must deliver one (1) **signed original** and one (1) **copy** of the Offer to Issuing Agency in a sealed package with Company Name and RFP Number clearly marked on the front. **The Vendor must return all the pages of this solicitation in their response.** The Vendor must also submit one (1) signed, executed electronic copy of its offer on a USB Flash Drive(s). The files should not be password-protected and should be capable of being copied to other media.

Address envelope and insert offer number as shown below. Please note that the US Postal Service does not deliver any mail (US Postal Express, Certified, Priority, Overnight, etc.) on a set delivery schedule to this Office. **It is the responsibility of the Vendor to have the offer in this Office by the specified time and date of opening.**

DELIVER TO:
OFFER NUMBER: ITS-400335 Department of Information Technology Attn: Kristen Burnette 3900 Wake Forest Road Raleigh, NC 27609

Sealed offers, subject to the conditions made a part hereof, will be received at 3900 Wake Forest Road, Raleigh, NC 27609 until 2:00pm Eastern Standard Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted in a sealed package with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed offer shall result in disqualification. All offers must comply with Section VI, Proposal Content and Organization.

Offers will not be accepted by electronic means. This RFP is available electronically at <https://www.ips.state.nc.us/ips/>. All inquiries regarding the RFP specifications or requirements are to be addressed to the contact person listed on Page One.

NON-RESPONSIVE OFFERS: Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

- "This offer does not constitute a binding offer",
- "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
- "The Vendor does not commit or bind itself to any terms and conditions by this submission",
- "This document and all associated documents are non-binding and shall be used for discussion purposes only",
- "This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties", or
- A statement of similar intent.

VENDOR LICENSE OR SUPPORT AGREEMENT(S): The terms and conditions of the Vendor's standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor's standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State's electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the DIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor's relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns; nor arbitrate any dispute, nor pay late fees, legal fees or other similar costs.

DIGITAL IMAGING: The State will digitize the Vendor's response if not received electronically, and any awarded contract together with associated contract documents. This electronic copy shall be a preservation record, and serve as the official record of this solicitation with the same force and effect as the original written documents comprising such record. Any printout or other output readable by sight shown to reflect such record accurately is an "original."

QUESTIONS CONCERNING RFP: Written questions concerning this RFP will be received until June 21, 2018 at 2:00pm Eastern Standard Time. They must be sent via e-mail to: Kristen Burnette@nc.gov. Please insert "Questions ITS-400335" as the subject for the email. The questions should be submitted in the following format:

Citation	Vendor Question	The State's Response
Offer Section, Page Number		

The State will prepare responses to all written questions submitted, and post an addendum to the Interactive Purchasing System (IPS) <https://www.ips.state.nc.us/ips/>. Oral answers are not binding on the State.

Vendor contact regarding this RFP with anyone other than Kristen Burnette may be grounds for rejection of said Vendor's offer.

ADDENDUM TO RFP: If a pre-offer conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State will be posted to the Interactive Purchasing System (IPS), <https://www.ips.state.nc.us/ips/>, and shall become an Addendum to this RFP. Vendors' questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State website for any and all Addenda that may be issued prior to the offer opening date.

BASIS FOR REJECTION: Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

NOTICE TO VENDORS: The State may, but will not be required to evaluate or consider any additional terms and conditions submitted with an Offeror's response. This applies to any language appearing in or attached to the document as part of the Offeror's response. By execution and delivery of this Invitation for Offer and response(s), the Offer agrees that any additional terms and conditions, whether submitted purposely or inadvertently, shall have no force or effect unless such are specifically accepted by the State.

LATE OFFERS: Regardless of cause, late offers will not be accepted and will automatically be disqualified from further consideration. It shall be the Vendor's sole risk to ensure delivery at the designated office by the designated time. Late offers will not be opened and may be returned to the Vendor at the expense of the Vendor or destroyed if requested.

VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM: The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following web site: <https://www.ips.state.nc.us/ips>

POINTS OF CONTACT: Contact by the Offeror with the persons shown below for contractual and technical matters related to this RFP is only permitted if expressly agreed to by the procurement officer named on page 2, or upon award of contract:

Vendor Contractual Point of Contact	Vendor Technical Point of Contact
[NAME OF VENDOR] Street: [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Contract Manager	[NAME OF VENDOR] Street: [STREET ADDRESS] [CITY, STATE, ZIP] Attn: Assigned Technical Lead

State Contractual Point of Contact	State Technical Point of Contact
North Carolina Department of Information Technology Statewide IT Procurement 3900 Wake Forest Road Raleigh, NC 27609 Attn: Kristen Burnette, Contract and Vendor Manager kristen.burnette@nc.gov	North Carolina Department of Information Technology 3700 Wake Forest Road Raleigh, NC 27609 Attn: Samila Mohseni, Enterprise Applications, Director samila.mohseni@nc.gov

Table of Contents

I. Introduction	6
II. Bidding Information	6
A. Procurement Schedule.....	6
B. Instructions to Vendors	7
C. General Conditions for Proposals	8
D. Evaluation Process	12
III. Technical Proposal	14
IV. Cost Proposal	31
V. Other Requirements and Special Terms	35
VI. Proposal Content and Organization.....	39
Attachment A. Attachments or Exhibits.....	42
Attachment B. Department of Information Technology Terms and Conditions.....	68

I. Introduction

The purpose of this Request for Proposal (RFP), and any resulting contract award, is for the North Carolina Department of Information Technology (NCDIT) on behalf of the State to solicit offers for an enterprise electronic forms and digital signature (EEF&DS) solution. Mandated by State Legislation, the awarded solution will replace North Carolina State Contract ITS006375 with a new multi-vendor/multi-solution statewide convenience contract. Contingent upon offer submissions, the State may choose to award one (1) or more Vendors as well as award multiple pricing models. The State's intent is to provide more than one cloud-based, software as a service (SaaS) solution that is responsive and cost effective to help state and local governments solve a wide variety of identity, authentication, confidentiality, data integrity, and non-repudiation (digital signatures) challenges. Multiple State agencies will leverage this contract, subsequently requiring the awarded vendor to invoice and provision each individual agency separately. Additionally, vendors should note that the State does require a rolled-up view of utilization both quarterly and yearly.

This state intends to award an *Indefinite Quantity Contract*, meaning this solicitation will establish a Contract pursuant to 9 NCAC 06B.0701 for an indefinite quantity contract between a vendor and the State. The quantity of goods or Services is undetermined. An estimated quantity based on past history or other means may be used as a guide, but shall not be a representation by the State of any anticipated purchase volume under any contract made pursuant to this solicitation.

In addition, the State reserves the right to make partial, progressive or multiple awards: where it is advantageous to award separately by items; or where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; and where other factors are deemed to be necessary or proper to the purchase in question.

II. Bidding Information

A. Procurement Schedule

The Procurement Manager will make every effort to adhere to the following schedule:

Action	Responsibility	Date
Issue of RFP	Statewide IT Procurement	6/11/2018
Deadline to Submit Additional Questions	Potential Vendors	6/21/2018
Response to Written Questions/RFP Amendments	Department of Information Technology	6/28/2018
Submission of Offer	Vendor(s)	7/12/2018

Action	Responsibility	Date
Offer Evaluation Complete	Evaluation Committee	7/26/2018
Oral Presentation and/or Product Demonstrations by Finalists (optional)	Vendors	8/2/2018
Negotiations (optional)	Evaluation Committee designees and selected Vendor(s)	8/14/2018
Best and Final Offers from Finalists (optional)	Vendors	8/23/2018
Contract Award	IT Procurement Office	8/30/2018
Protest Deadline	Vendors	15 days after award

B. Instructions to Vendors

Additional acronyms, definitions and abbreviations may be included in the text of the RFP.

- 1) Offers submitted electronically, or via facsimile (FAX) machine will not be accepted.
- 2) **EXECUTION:** Failure to sign under EXECUTION section will render offer invalid.
- 3) **PROMPT PAYMENT DISCOUNTS:** Vendors are urged to compute all discounts into the price offered. If a prompt payment discount is offered, it will not be considered in the award of the Agreement except as a factor to aid in resolving cases of identical prices.
- 4) **MISCELLANEOUS:** Masculine pronouns shall be read to include feminine pronouns and the singular of any word or phrase shall be read to include the plural and vice versa.
- 5) **VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM:** Electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available on the Interactive Purchasing System at the following web site: <https://vendor.ncgov.com/vendor/login>
- 6) **ORGANIZATION:** Vendors are directed to carefully review Section VI herein and fully comply with the content and organizational requirements therein.
- 7) **E-PROCUREMENT:** This is not an E-Procurement solicitation. See paragraph #33 of the attached North Carolina Department of Information Technology Terms and Conditions Services made part of this solicitation contain language necessary for the implementation of North Carolina's statewide E-Procurement initiative. It is the Vendor's responsibility to read

these terms and conditions carefully and to consider them in preparing the offer. By signature, the Vendor acknowledges acceptance of all terms and conditions including those related to E-Procurement.

- a) General information on the E-Procurement service can be found at <http://eprocurement.nc.gov/>
 - b) Within two days after notification of award of a contract, the Vendor must register in NC E-Procurement @ Your Service at the following web site: <http://eprocurement.nc.gov/Vendor.html>
 - c) As of the RFP submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this RFP.
 - d) If the awarded Vendor does not stay current on all E-Procurement fees, the State may remove the Vendor from the Agreement for a thirty (30) calendar day period or until resolution, whichever is shorter. If the Vendor is making a reasonable effort to resolve any past due fees, no penalty will be imposed. The determination of the reasonable effort criteria will be at the discretion of the Statewide IT Procurement Office.
- 8) **E-VERIFY:** Pursuant to N.C.G.S. §143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.
- 9) **RESTRICTIONS ON CONTRACTS WITH THE STATE:** Reserved

C. General Conditions for Proposals

- 1) **DEFINITIONS, ACRONYMS AND ABBREVIATIONS:** Generally, see 9 NCAC 06A.0102 for definitions. The following are additional defined terms:
- a) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
 - b) **ADA:** Americans with Disabilities Act
 - c) **APIs:** Application Programming Interfaces
 - d) **BAA:** Business Associates Agreement
 - e) **CRM:** Customer Relationship Management
 - f) **CSV:** Comma Separated Values
 - g) **Deliverables:** Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include "Work Product" and means any expression of Licensor's findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.

- h) **EEF&DS:** Enterprise Electronic Forms and Digital Signature
 - i) **FERPA:** Family Educational Rights & Privacy Act
 - j) **Goods:** Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
 - k) **HIPAA:** Health Insurance Portability and Accountability Act
 - l) **IaaS:** Infrastructure as a Service
 - m) **IDM:** Identity Management
 - n) **LDAP:** Lightweight Directory Access Protocol
 - o) **NCID:** North Carolina Identity Service
 - p) **NCDIT or DIT:** The NC Department of Information Technology, formerly Office of Information Technology Services.
 - e) **ODBC:** Open Database Connectivity.
 - f) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
 - g) **PaaS:** Platform as a Service
 - h) **PII:** Personal Identifiable Information
 - i) **PCI:** Payment Card Industry
 - j) **Reasonable, Necessary or Proper:** as used herein shall be interpreted solely by the State of North Carolina.
 - k) **RFP:** Request for Proposal
 - l) **RPO:** Recovery Point Objective
 - m) **RTO:** Recovery Time Objective
 - n) **SaaS:** Software as a Service
 - o) **SLA:** Service Level Agreement
 - p) **SAP/SAP SSO:** Systems, Applications, and Products/ SAP Single Sign On
 - q) **The State:** Is the State of North Carolina, and its Agencies.
 - r) **Transaction:** Workflow package requiring one or more e-signatures.
 - s) **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.
 - t) **WSI:** Web Services Interoperability
 - u) **NIEM:** National Information Exchange Model
- 2) **READ AND REVIEW:** It shall be the Vendor’s responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications and the State’s intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State’s contact person listed on the front page of the solicitation. Questions and clarifications must be submitted in writing and may be submitted by personal delivery, letter, fax or e-mail within the time period identified hereinabove.
- 3) **VENDOR RESPONSIBILITY:** The Vendor(s) will be responsible for investigating and recommending the most effective and efficient technical configuration for any online services. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the recommended approach is not short lived. The Vendor(s) must provide a justification for their proposed online services solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value

added Services or other criteria identified herein. The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor. The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

- 4) **ELIGIBLE VENDOR:** The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), the Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).
- 5) **ORAL EXPLANATIONS:** The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendor contact regarding this RFP with anyone other than the Agency contact or procurement officer named on Page 1 above may be grounds for rejection of said Vendor's offer. Agency contact regarding this RFP with any Vendor may be grounds for cancellation of this RFP.
- 6) **INSUFFICIENCY OF REFERENCES TO OTHER DATA:** Only information that is received in response to this RFP will be evaluated. Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation.
- 7) **CONFLICT OF INTEREST:** Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.
- 8) **CONTRACT TERM:** A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The term shall be **Three (3)** years, and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for **two (2)** additional **one (1)** year periods at its sole discretion.
- 9) **EFFECTIVE DATE:** This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the State until the appropriate State purchasing authority/official or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for Services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.
- 10) **RECYCLING AND SOURCE REDUCTION:** Reserved.

- 11) **HISTORICALLY UNDERUTILIZED BUSINESSES:** Pursuant to N.C.G.S. §§143B-1361(a), 143-48 and 143-128.4 and any applicable Executive Order, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. Additional information may be found at: <http://ncadmin.nc.gov/businesses/hub/>.
- 12) **CLARIFICATIONS/INTERPRETATIONS:** Any and all amendments or revisions to this document shall be made by written addendum from the DIT Procurement Office. Vendors may call the purchasing agent listed on the first page of this document to obtain a verbal status of contract award. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.
- 13) **RIGHTS RESERVED:** While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:
- a) waive any formality;
 - b) amend the solicitation;
 - c) cancel or terminate this RFP;
 - d) reject any or all offers received in response to this RFP;
 - e) waive any undesirable, inconsequential, or inconsistent provisions of this RFP;
 - f) if the response to this solicitation demonstrate a lack of competition, negotiate directly with one or more Vendors;
 - g) not award, or if awarded, terminate any contract if the State determines adequate State funds are not available;
 - h) if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply 09 NCAC 06B.0316 (c); or
 - i) negotiate with one or more Vendors under 09 NCAC 06B.0316 (b).
- 14) **ALTERNATE OFFERS:** The Vendor may submit alternate offers for various levels of Service(s) meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s) addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services and offer at specific pricing. If a Vendor chooses to respond with various Services offerings, each must be an offer with a different price and a separate RFP offer.

Alternate offers must be clearly marked
“Alternate Offer for ‘name of Vendor’”

and numbered sequentially with the first offer if separate offers are submitted. This legend must be in bold type of not less than 14-point type on the face of the offer, and on the text of the alternative offer.

- 15) **CO-VENDORS:** Vendors may submit offers as partnerships or other business entities. Such partners or other “co-Vendors”, if any, shall disclose their

relationship fully to the State. The State shall not be obligated to contract with more than one Vendor. Any requirements for references, financial statements or similar reference materials shall mean **all** such partners or co-Vendors.

- 16) **SUBMITTING AN OFFER:** Each Vendor submitting an offer warrants and represents that:
 - a) The offer is based upon an understanding of the specifications and requirements described in this RFP.
 - b) Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.
- 17) **SUBMITTED MATERIALS:** All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.
- 18) **MODIFICATIONS TO OFFER:** An offer may not be unilaterally modified by the Vendor.

D. Evaluation Process

- 1) **BEST VALUE:** "Best Value" procurement methods are authorized by N.C.G.S. §§143-135.9 and 143B-1350(h). The award decision is made based on multiple factors, including: total cost of ownership, meaning the cost of acquiring, operating, maintaining, and supporting a product or service over its projected lifetime; the evaluated technical merit of the Vendor's offer; the Vendor's past performance; and the evaluated probability of performing the specifications stated in the solicitation on time, with high quality, and in a manner that accomplishes the stated business objectives and maintains industry standards compliance. The intent of "Best Value" Information Technology procurement is to enable Vendors to offer and the Agency to select the most appropriate solution to meet the business objectives defined in the solicitation and to keep all parties focused on the desired outcome of a procurement. Evaluation shall also include compliance with information technology project management policies, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation.
- 2) **SOURCE SELECTION:** A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value, and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with, or traded-off against other non-price factors.
 - a) The evaluation committee may request clarifications, an interview with or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, the response to a clarification request given by any Vendor. Vendors are cautioned that the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should

be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer.

- b) Evaluation Process Explanation. State Agency employees will review all offers. All offers will be initially classified as being responsive or non-responsive. If an offer is found non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.
 - c) To be eligible for consideration, a Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to any one factor may be grounds for rejection regardless of overall score.
 - d) Vendors are advised that the State is not obligated to ask for, or accept after the closing date for receipt of offer, data that is essential for a complete and thorough evaluation of the offer.
- 3) **BEST AND FINAL OFFERS (BAFO):** If negotiations or subsequent offers are solicited, the Vendors shall provide BAFOs in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State may establish a competitive range based upon evaluations of offers, and request BAFOs from the Vendors within this range; e.g. "Finalist Vendors". The State will evaluate BAFOs and add any additional weight to the Vendors' respective offer. Additional weight awarded from oral presentations and product demonstrations during negotiations, if any, will be added to the previously assigned weights to attain their final ranking.
- 4) **EVALUATION CRITERIA:** Each of the criteria below shall be evaluated in accordance with the solicitation documents:
- a) **Corporate Background and Experience:** Vendor's corporate background and similar experience specifically relevant to the technical situations, specifications, needs, challenges, and opportunities as presented in this RFP.
 - b) **Technical Approach:** Substantial Conformity to Solicitation Requirements and Specifications;
 - i. Effectiveness of approaches, designs, services, processes, and practices as they relate to the solution.
 - ii. Illustration(s) and/or explanations of the Statewide Technical Architecture objectives, principles and best practices to the proposed solution.
 - c) **Proposed Approach and Schedule:** Proposed approach and schedule of work to be performed. This encompasses areas such as producing acceptable deliverables; organization, timing, and structure of work activities in accordance with any stated timeframes.
 - d) **Total Cost of Ownership:** The cost of acquiring, operating, maintaining, and supporting a product or service over its projected lifetime.

- 5) **PAST PERFORMANCE:** Vendor may be disqualified from any evaluation or award if Vendor or any key personnel proposed, has previously failed to perform satisfactorily during the performance of any contract with the State, or violated rules or statutes applicable to public bidding in the State.
- 6) **EVALUATION METHOD:** This procurement will be evaluation in accordance with the Narrative method.
- 7) **INTERACTIVE PURCHASING SYSTEM (IPS):** The State has implemented links to the Interactive Purchasing System (IPS) that allow the public to retrieve offer award information electronically from our Internet web site: <https://www.ips.state.nc.us/ips/>. Click on the IPS BIDS icon, click on Search for BID, enter the Agency prefix-offer number (XXXX), and then search. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.
- 8) **PROTEST PROCEDURES:** Protests of awards exceeding \$25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in this office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests will be governed by Title 9, Department of Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**

III. Technical Proposal

- 1) **ENTERPRISE ARCHITECTURE STANDARDS:** The North Carolina Statewide Technical Architecture is located at the following website: (<https://it.nc.gov/services/it-architecture/statewide-architecture-framework>). This provides a series of domain documents describing objectives, principles and best practices for the development, implementation, and integration of business systems. Agencies and Vendors should refer to these Architecture documents when implementing enterprise applications and/or infrastructure.
- 2) **ENTERPRISE LICENSING:** In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements. The agreements may be viewed at: <http://it.nc.gov/services/license-and-agreements>
 - a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.
 - b) Identify and explain any components that are missing from the State's existing license agreement.
 - c) If the Vendor can provide a more cost effective licensing agreement, please explain in detail the agreement and how it would benefit the State.
 - d) Explain the transportability and transferability of the proposed license agreements. Any licenses or warranties purchased on behalf of the State for this project must be transferable at the time the Vendor is paid under contract for said component
- 3) **VIRTUALIZATION:** *Reserved*

- 4) **NCID:** Reserved.
- 5) **CLOUD SERVICE PROVIDERS (CSPs):** For offers featuring a cloud-hosted solution, Vendors shall describe how the proposed solution will support the agency's information system security compliance requirements as described in the Statewide Information Security Manual, specifically relating to, and without limitation, the sections relating to cloud services: <http://it.nc.gov/statewide-resources/policies>. *The [e-Forms/e-Signature Program](#) should be classified as NIST Moderate per the Statewide Information Security Manual and will be required to receive and securely manage data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy.* To comply with policy, State agencies are required to perform annual security/risk assessments on their information systems using NIST 800-53 controls. This requirement additionally applies to all vendor provided, agency managed Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions. Assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.
- 6) **BRANDING:** All offers that incorporate State design and branding, as specified by the State, shall adhere to the State style guide. The State style guide is located at: <http://digitalstyle.nc.gov>.
- 7) **EQUIVALENT ITEMS:** Reserved.
- 8) **LITERATURE:** All offers shall include specifications and technical literature sufficient to allow the State to determine that the proposed solution substantially meets all specifications. This technical literature will be the primary source for evaluation. If a specification is not addressed in the technical literature it must be supported by additional documentation and included with the offer. Offer responses without sufficient technical documentation may be rejected.
- 9) **EQUIVALENT GOODS:** Reserved.
- 10) **DEVIATION FROM SPECIFICATIONS:** Any deviation from specifications indicated herein must be clearly identified as an exception and listed on a separate page labeled "Exceptions to Specification." Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.**
- 11) **SCOPE OF WORK:**
In 2013, the General Assembly transferred the responsibility of procuring electronic forms and digital signature services from the Office of the State Controller (OSC) to the Department of Information Technology (DIT) and the agency's State CIO. Thereby, per North Carolina State Legislation, the

awarded solution must adhere to several technical requirements (**Please see Section III, #12.**)

The following language is taken directly from the North Carolina statute:

The proposed digital solution shall adhere to the N.C. Uniform Electronic Transactions Act (NCGS 66311), the Federal Electronic Signatures in Global and National Commerce Act (Title 15), NC eCommerce (NCGS 66-58.12), NC Cash Management Statute (NCGS 147.86-22(b)), and the Electronic Notary Act (Chapter 10B, Article 2) and the N.C. Electronic Notary Standards (18 NCAC 07C) § 66-58.4. Use of electronic signatures.

All public agencies may use and accept electronic signatures pursuant to this Article, pursuant to Article 40 of this Chapter (the Uniform Electronic Transactions Act), or pursuant to other law. (1998-127, s. 1; 2003-233, s. 1; 2007-119, s. 1.)

Based on current usage, the State estimates that the solution will eventually accommodate over 95,000 transactions. The State will proceed with a decentralized approach of the program with minimal central management of the enterprise form and digital signature solution. This approach will allow the State to enter into contracts with vendors and allow agencies to access services as they need them for the most cost-effective price. Therefore, in addition to solving a wide variety of identity, authentication, confidentiality, data integrity, and non-repudiation (digital signatures) challenges, any vendor partnerships must invoice and provision each individual agency separately.

12) **TECHNICAL REQUIREMENTS:**

In accordance with the legislative mandate, the awarded solution must conform with the following requirements. Vendors should read the information regarding each requirement and any corresponding reference, and provide detailed answers when prompted. Note: *Solutions not adhering to technical requirements will not be considered by the State.*

a) **PII (Personal Identifiable Information)**

N.C. Gen. Stat. §75-61(10) defines personal identifying information (PII), in part, as “[a] person’s first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b),” and “identifying information” is defined by G.S. § 14-113.20(b) to include Social Security Number or employer taxpayer identification numbers, Driver’s License, State Identification Card, or Passport Numbers, Checking Account Numbers, Savings Account Numbers, Credit Card Numbers, Debit Card Numbers, Personal Identification (PIN) Code as defined in G.S. § 14-113.8(6), Electronic identification numbers, electronic mail names or addresses, internet account numbers, or Internet identification names, Digital Signatures, any other numbers or information that can be used to access a person’s financial resources, Biometric Data, Fingerprints, Passwords and Parents’ legal surnames prior to marriage. **Proposed solutions must adhere to PII protection laws.**

Therefore, please describe how the solution is PII compliant.

b) HIPAA (Health Insurance Portability and Accountability Act)

The Contractor agrees that, if the Division determines that some or all of the activities within the scope of this contract are subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-91, as amended ("HIPAA"), or its implementing regulations, it will comply with the HIPAA requirements and will execute such agreements and practices as the Division may require to ensure compliance. HIPAA forms, instructions and other materials can be located on the HIPAA web site: <http://hipaa.dhhs.state.nc.us/index.html>. **If applicable, proposed solutions must adhere to HIPAA laws.**

In consideration of this requirement, please describe how the proposed solution is HIPAA compliant. Please note that the State requires a business associates agreement (BAA).

c) PCI (Payment Card Industry)

The Payment Card Industry (PCI) Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

In consideration of this requirement, please describe how the proposed solution is PCI compliant.

d) FERPA (Family Educational Rights & Privacy Act)

The Family Educational Rights & Privacy Act (FERPA) states that student educational records are subject to 20 U.S.C. 1232g, Family Rights and Privacy Act (FERPA). Therefore, the Vendor must ensure that the proposed solution fully complies with FERPA and every employee responsible for carrying out the terms of this contract is aware of the confidentiality requirements of federal law. In addition, every such employee must sign a confidentiality acknowledgement that indicates that he or she understands the legal requirements for confidentiality. The Vendor is responsible for the actions of its employee and must take all precautions necessary to ensure that no violations occur. Finally, access to personally identifiable student education information shall be limited to those employees who must have access to it in order to perform their responsibilities pursuant to this contract.

In compliance with the law, please describe the following:

1. Describe the capabilities of tracking and reporting the application access.
2. Describe the solution's approach to handling non-public data at rest and non-public data in motion.
3. Describe the solution's approach for encrypting data such that only the intended recipient can decrypt it.
4. Describe the solution's process for handling and notification of a breach of non-public data.
5. For authorization, describe the solution's handling of various roles associated with data access.

e) **Security**

The state potentially handles a large amount of non-public data. **Proposed solutions must adhere to North Carolina Statewide IT Security Policies and Standards (<https://it.nc.gov/statewide-information-security-policies>)**, as they may relate to personal and/or confidential data. Therefore, please address the following:

The State also requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). **Attachment B** provides a high-level view of specific security requirements that are requirements to meet compliance. Vendors must fill out the **VENDOR ASSESSMENT GUIDE in Attachment B**.

Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates.

The following items are security and/or solution requirements; therefore, describe how the solution will accommodate the following:

1. The solution must alert the user to any changes to a document after a digital signature has been applied.
2. The digital signature service component must require users to prove their identity before applying an electronic signature to a document.
3. The solution must provide digital certificates to establish non-reputation (i.e. cannot deny receipt or signature).
4. The solution must provide digital hashes to establish fixity (i.e. guarantees that digital documents have not been altered since completion).

- 13) **TECHNICAL SPECIFICATIONS**: Means, as used herein, a specification that documents the requirements of a system or system component. It typically includes functional requirements, performance requirements, interface requirements, design requirements, development standards, maintenance

standards, or similar terms. Substantial conformity with technical specifications is required.

- a) **Site and System Preparation:** Vendors shall provide the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. The Vendor shall advise the State of any site requirements for any Deliverables required by the State's specifications. Any alterations or modification in site preparation which are directly attributable to incomplete or erroneous specifications provided by the Vendor and which would involve additional expenses to the State, shall be made at the expense of the Vendor.
- b) **Specifications:** The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and only processes, configuration, material and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified. See, Acceptance Criteria, below.
- c) **Directions:** Please describe how the proposed solution will meet the following technical specifications, including capabilities, features, and limitations. *Note: Vendors are encouraged to align responses with the technical specifications' outline shown below.*

1. General Features

Provide the general features of the proposed solution. Please include the following information:

- a. Use this prompt to articulate an understanding of the state's need as well as any value-added services relevant to this RFP.
- b. Address the solution's capacity to include ad hoc workflow routing rules, based on unique business rules defined for document(s) and signature requirements.
- c. Can the solution deliver business process workflow for documents, from originator to signatories?
- d. Can the solution integrate with global address books or pull users into a centralized address book?
- e. Address whether the solution will permit external party signing, including two-factor or multi-factor authentication. Provide examples.
- f. Describe the capability to establish evidentiary requirements for signed documents.
- g. Describe the process of creating new forms and templates.

- h. Address whether each person in the workflow is given the opportunity to review all documents, with confirmation opportunity, before the transaction continues.
- i. The State needs the signing process to be simple, and require very few steps for users. The steps required to secure signatures should not become more burdensome for any staff involved than current paper processes. Therefore, describe if the solution configures predefined workflow routing rules based on specific business rules defined for document(s) and signature requirements.
- j. Describe the solution's capacity to store completed, digitally signed document(s), on the State's own Document Management System; Include whether the:
 - Solution supports grouping and/or compartmentalization of originators (i.e. by department, function, division, section) so that documents may not be visible to disparate workgroups.
 - Originators monitor the progress and status of transactions they and/or their workgroups have initiated.
- k. Describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.
- l. Describe if the solution facilitates digital signing of documents on IOS, Android, and Windows smart phones. Specify minimum software versions supported.
- m. Also include whether the solution facilitates digital signing of documents on IOS, Android, and Windows mobile tablet devices. Specify minimum software versions supported.
- n. Address if the solution can create and manage multiple levels of system access.
- o. Describe if the solution will provide a copy of record for the electronic document, sufficient to prove, in private litigation, civil enforcement proceedings, and criminal proceedings, that: (1) the electronic document was not altered without detection during transmission or at any time after receipt; (2) any alterations to the electronic document during transmission or after receipt are fully documented.
- p. Clarify that the solution disallows any form of unauthorized copying or pasting signatures.
- q. Describe if the solution will determine if any modifications were made after the signature for the relevant sections were attached and disallow modifications or invalidate corresponding section that was modified.
- r. Explain if the solution will contain the copy of record, which will include
 - All electronic signatures contained in or logically associated with that document.
 - The date and time of receipt.
 - Any other information used to record the meaning of the document or the circumstances of its receipt.
 - Other, such as authorized system ID of signature owner, authorized computer ID, smart device ID such as MAC address, location data, etc.

- Detection of unauthorized data modification and place obvious marker on the document – electronic version and paper version.
- A function to alert users of needed actions.

2. Product Strategy Roadmap

The state needs a fully-developed plan Provide a 12-month Vendor product strategy as it relates to the solution proposed.

3. Disaster Recovery and Hosting Facilities

The state needs to understand the hosting facilities, capabilities and disaster recovery capabilities of the proposed solution, and requires an application disaster recovery plan as well. In addition to these needs, please address the following:

- Explain how the vendor will work with the state to develop this plan and integrate it with agency operation.
- The data that is stored in this application's database may be confidential and if so, must follow HIPAA, FERPA, PII and PCI compliance. Explain how the vendor will protect this data in the case of an event that requires execution of the disaster recovery plan.
- Describe the hosting facilities. Use diagrams where appropriate. Consider the following aspects:
 - Who is the hosting provider? Where is the primary site? Where is the disaster recovery site?
 - Explain if the hosting facilities are SAS 70 II compliant and/or compliant with SSAE 16 reporting standards, please provide copies of the most recent audit(s).
 - What is the data center's classification (Tier 1, Tier 2 etc.)?
 - What policies are in place to thwart insider breaches?
 - What is the process for background checks? Who are they performed by, for which employees, are the checks performed at employment, yearly, etc.
 - Will all customer data be housed within the continental United States?
 - Are there any circumstances when the solution would store customer data and intellectual property outside of the United States or with a non-USA owned institute?

4. Data Management

- Describe how data is archived and/or purged.
- The State must receive an attestation letter explaining how the Vendor destroyed the data when the State separates

from the Vendor. Please acknowledge that the solution will supply such communication.

- c. Describe how the state will get its data back in a form that can be used. What costs will be involved if any?
- d. How is the data destroyed at the end of a term contract?
 - Address how workflows, meta-data and configurations will be transferred to the state.

5. Audit

The state retains the right to audit the physical environment (could apply to production, secondary site, etc.) where the vendor application/service is hosted per the vendor proposal. Therefore, describe what processes the solution has in place to allow this audit?

- a. Describe if the solution will provide a retrievable audit trail.
- b. Supply the chain of custody for obtaining the record of copy.
- c. Address if the solution can export capabilities for the audit trail data. List possible export formats.
- d. Describe if audit event details are available to customer in a reusable format (i.e. CSV, Excel, PDF).
- e. Describe how the Audit trail is stored and secured against tampering.
- f. The solution must track every event in the signature process. Therefore, describe to what degree such details and events are being stored.
- g. Explain how consent from users to use the service is tracked as an auditable action.

6. NCID

For Identity Management, the state has invested in a common solution called NCID. NCID is the State's enterprise identity management (IDM) service and is operated by the North Carolina Office of Information Technology Services. (The details of NCID can be found at: <https://it.nc.gov/ncid/>.) Additional information regarding this service can be found in the ITS Service Catalog at: <http://www.its.state.nc.us/ServiceCatalog/Index.asp> (see Identity Management - NC Identity Management under the main menu item Application Services).

In consideration of this environment, describe the solution's capabilities to integrate with NCID. Also, explain the solution's capability to externalize NCID. Within **Section IV. Cost Proposal**, include an estimate to integrate NCID with the proposed solution understanding that this is a decentralized solution and will be invoiced by the individual agencies.

Please also address the following:

- a. Describe how the solution handles varying roles for authorization. Such as guest account (citizen non-authenticated), administrators, etc.
- b. The state seeks to achieve reduced or simplified sign-on capabilities. Describe how the solution supports reduced or simplified sign-on.
- c. It is possible that there will exist multiple identity stores or vaults. Explain the solution's capacity to handle federated identity.

7. Architecture

The state prefers a cloud-based, software as a service (SaaS) solution; therefore, please address the following:

- a. What is the solution's SaaS architecture model?
- b. Provide examples of scalability for very large organizations and numbers of concurrent and daily transactions.
- c. Describe how the application performs under load, both in terms of number the number of users and the transaction volume.
- d. Does the application dynamically scale based on runtime usage and demand?
- e. Provide details to further demonstrate that the proposed architecture and supported platform will scale to meet State current peak and future application processing and user demand.
- f. Describe the proposed solution's applications architecture, including offline capabilities, multi-language support, and interface standard supported.
- g. Describe the solution as related to smart devices and operations on smart devices including but not limited to smart pads, smart phones on various platforms. Include limitations in functionality, security, need for installation of facilitating software (apps) and possible additional costs.

8. Interoperability and Integration

The proposed solution may be required to interface with a variety of other systems. In consideration of this need, respond to the following:

- a. Please describe in detail what type of integration the solution supports; i.e., the integration architecture.
- b. Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided. Some of the potential integrations are:
 - SAP (SAP SSO cookies for example)
 - Web services (MQ Series, other APIs)
 - Enterprise Service Bus (e.g. Web Sphere Service Broker)
 - LDAP (for authentication)
 - NCID (for identity management)

- Document management systems (list)
 - Office software packages (Office 365)
 - Business systems such as human resources, accounting, finance, CRM, ERP, LMS, etc.
 - SharePoint Online and On Premises
 - Dynamics 365, Salesforce.com
- c. Are APIs secure and encrypted? What Encryption Method,
 - d. How do you extract form or record data? Do you use industry standards such as XML?
 - e. How is data inserted into a form? Can data be inserted dynamically (based on user inserted data)?
 - f. Can forms be processed via API in both real time and/or batch mode?
 - g. How does the API deal with multiple accounts (for enterprise-wide forms)?
 - h. Can the API retrieve software version numbers?
 - i. How are fields identified in the API?
 - j. How is the workflow engine capable of easily supporting a variety of e-forms?
 - k. The state prefers REST web service interfaces. XML schemas should be derived from industry standard vocabularies where possible such as the National Information Exchange Model (NIEM). Describe how the solution will support these and other interoperability standards.

9. Applications Management and Control

Describe the process of raising and managing exceptions within the application. Please include the following:

- a. Address whether multifactor authentication (MFA) access is available for all accounts including signatories, admins, and form builders? Is it included in the price? If not provide pricing in the cost section.
- b. Describe the level of customer control on the timing of applying patches, upgrades, and changes to the SaaS application and the notification process to be used.
- c. Explain the process for handling software defects.
- d. Describe the major and minor release policy for the solution.
- e. Describe user configuration capabilities.
- f. Describe user self-provisioning capabilities.
- g. Describe the level and skill set needed by the State to administer and configure the proposed solution.
- h. How do you address Delegation of authority?
- i. Describe how privileged management accounts are secured, provide encrypted authentication and access to authorized users.

- j. Specifically, does the Delegation of Authority capability that allows signatories to delegate signing authority for documents for a specified period of time, or indefinitely.

10. Application Specifications

Please describe how the solution will include the following application specifications:

- a. Describe integration with Microsoft Office 365 Office Productivity & Email.
- b. Describe how the solution can initiate the signature process with PDF and Word documents. *Please note that the vendor may apply custom branding (official logos, colors, hyperlinks) as necessary to create a consistent user experience. Please see **Section III, #6** for more information.*
- c. Describe how the solution works with Section 508 compliant screen readers and other ADA capabilities. Specifically, in-process and completed documents should be fully read by a screen reader.
- d. Provides a digital signature solution in which the "root" digital certificate is provided by a certificate authority that meets assurance and trust requirements by Adobe. Documents with these certificates become automatically trusted by Adobe as this facilitates the ability to validate the signature. More information about Adobe's Approved Trust List and current members of that list can be found at <http://helpx.adobe.com/acrobat/kb/approved-trust-list2.html>.
- e. Provides the ability for anyone to open a digitally signed PDF and observe a signature validity confirmation across the top of the file that indicates all signatures are signed and valid.
- f. Users of the e-signature service are given an opportunity to decline to use the service.
- g. Does the solution provide the capability for electronic notarization.
- h. Digital signature notifications are achievable through SMTP relay, direct email client integration (i.e. "mailto:"), or SMS (text messages). Please describe these and/or other capabilities.
- i. Describe what notifications are sent to a user for signature?
- j. Please describe the solution's policy for handling customer's intellectual property, data, and information.
- k. Describe if the solution can import a predefined electronic list (i.e. CSV, ODBC, Excel) of customer's vendors and business partners. Please describe capability and any limitations that may exist.

11. Automation of Forms

Explain how the solution will address the automation of forms.
Provide an explanation regarding the:

- a. Process for integrating field validation (both data and format).
- b. Process for database integration.
- c. The limitations on the number of standard templates that can exist.
- d. Level at which standard templates exist – whole org., division, etc? Provide examples.
- e. Revision process to forms without customization from vendor.
- f. Use of existing form templates created by other products.
- g. Methodology regarding how calculations are conducted within form.
- h. Process for creating and publishing forms to agency websites.
- i. Process required for citizens to use forms posted to Agency websites via the solution.
- j. Methodology regarding how persons in a workflow can redline data in a form that is in process and route that form back to the originator for revision. Describe the form data capture – stored in form replica and/or recreated from database and ability to extract either way.
- k. Process for pre-populating user specific information such as name, address, and etc.
- l. Solution's method for marking sections of the document where signature is required.
- m. Solution will allow forms to be labeled by type of process, such as HR, Finance, Payroll, etc.

12. Workflow

Describe the solution's workflow capabilities. Include the functionalities below within the description:

- a. Provide examples of templates for developing workflows per the solution that will standardize business engineering processes and improve workflow development efficiency.
- b. Any limitations to the size of documents sent through workflow.
- c. Any limitations to the combined file size of a transaction with multiple files attached.
- d. Each person in the workflow is given the opportunity to review all documents, with a confirmation opportunity, before the transaction continues.
- e. The solution allows for rejection. If a form is rejected, specify how commenting, rerouting, markup of document is allowed.
- f. The solution supports the approving/rejecting of multiple sections of a document by more than one approver and/or signer.
- g. Workflows are setup based on Roles and Permissions

- h. User initiates signing.
- i. Each department/division/unit can have and maintain their own customizable workflows.
- j. Routing of multiple types of documents with multiple signatures within a single transaction.
- k. Users can track the progress of a transaction – including stage and status.
- l. The process for copying previously created workflows
- m. The solution generates a diagram of the workflow.
- n. User can abandon signing a document.
- o. Portions of the workflow that are configurable by the Department/Division/Unit.
- p. Queues are established to assist users to process, review, analyze and approve depending on role.
- q. Support Ad Hoc signing from cloud and smart devices.
- r. Workflow creation can be automated. (i.e. – Roles copied from other systems such as HR/Payroll systems).
- s. Documents which do not require signature are bound to signature documents and routed through the workflow.
- t. Workflow can be redirected and users injected to the flow.
- u. Support branding and color scheme customization of document packages for signature.
- v. Support document creator workflow rerouting with and without workflow start over.
- w. How an external system process can be added as a workflow step/approval.
- x. Describe how the solution will generate workflow and forms meta-data and the content of such meta-data specifying what is included, and what is excluded.

13. Signature/Initialing

Describe the solution's signature and initialing capabilities. Include how the:

- a. Digital signature is linked to the documents being signed. Describe how this is achieved.
- b. Solution assigns and restricts the sole control of the signature to the owner.
- c. Solution captures the users "actual" signature and initials.
- d. Solution captures a picture of the signature owner and associates it with the actual signature.
- e. Solution captures speed, pressure and x-y coordinates of signatures.
- f. Receiver of data can determine origin.
- g. Electronic document cannot be altered without detection at any time after being signed.
- h. Code or other mechanism is used to create digital signatures and how that code or mechanism is unique to that individual at the time of signature.

14. Repudiation

Describe how the solution addresses repudiation; specifically address how the solution will provide:

- a. True and correct copy of document received – provide sufficient evidence to show how the copy of record was derived from and accurately reflects the electronic document as it was received by the system, this evidence is also necessary to establish document integrity.
- b. A human-readable format that clearly and accurately associates all the information provided in electronic document with descriptions or labeling of the information and provides the opportunity to repudiate the electronic document based on this review.
- c. Inclusion of other information necessary to record meaning of document – such as data field labels, signatory information such as references to validation mechanism, and transmission source information.
- d. Procedures to address submitter/signatory repudiation of a copy of record.
- e. Confirmation of receipt of intact form data or record.
- f. Expunging of transaction upon authorized request.
- g. Long term validation of electronically signed document. Describe how electronically signed document will maintain validity for long term (multiple years out).

15. Notification

Describe the solution's notification capabilities, include if the solution:

- a. Provides opportunity to review certification statements and warnings (including any applicable certifications that false certification carries criminal penalties).
- b. Provides notification that copy of record is available and this notification is configurable by each Department/Division/Unit.
- c. Flags accidental submissions.
- d. Supports setting expirations and notifications.
- e. Has expirations and notifications that can be set for a standard (e.g. three-month expiry) for whole organization, a division, and individual and etc.
- f. Makes it clear that the signed document represents a completed declaration of will, and not just a draft which the signatory did not intend to be bound by – Finality function.
- g. Makes a signatory aware that by his/her signature he/she is entering into a binding transaction – Cautionary function.
- h. Includes automatic acknowledgement of receipt.

16. Storage

Describe the following storage capabilities; include if the solutions storage functionality can:

- a. To print or store locally by person(s) in the process.
- b. Form data or record will be stored – vendor or agency.
- c. Provide costs estimate for vendor storage in **Section IV**.
Provide cost estimate for any transmission cost if stored at agency in **Section IV**.
- d. Store and accommodate according to each department/division/unit record retention and disposition schedule.
- e. Allow procedures for retrieving documents from Vendor; during contract term.
- f. Allow procedures for retrieving documents from Vendor; expired contract term.
- g. Format documents are received and stored in.
- h. Support document package labeling for ease of segmented document storage outside of the native solution data center
- i. Process for retrieving information required to meet eDiscovery requests when documents are stored at a Vendor operated or controlled site; or when information retrieval requires participation of the Vendor or a third party.
- j. Process for searching and sorting information stored at Agency site to meet eDiscovery requests (e.g. – record identifiers).
- k. Exit Strategy –Define how this process would work and what costs would be involved. Is there a cost for transferred data?

17. **Service Level Agreement (SLA) and Reporting**

The ideal solution will have a detailed Service Level Agreement (SLA)

- a. Provide a copy of the proposed Service Level Agreement (SLA). Including notation of optional levels of service and Breaches in SLA from a Financial standpoint.
- b. What is the standard service availability that the solution commits to provide in a Service Level Agreement (SLA)? Please provide quantitative response in percentage (%) and any other details to describe this service availability commitment.
- c. Is the SLA Financially backed?
- d. With respect to RPO and RTO, please describe how the solution provided allows for an RPO of 24 hours and an RTO of 24-48 hours. Describe the architectural approach, infrastructure and operating environment that are necessary to meet the stated recovery point and time objectives. In addition, tell us if the proposed solution exceeds those metrics.
- e. Describe report and metrics generation capabilities. Show examples of how utilization can be tracked by user or groups of users.

- f. The state will require a rolled-up view of all usage broken down by agency quarterly and yearly; therefore, describe how the solution will allow agencies to run their own usage reports.
- g. The total transaction volume can be tracked by month, by Department/Division/Unit, and reported to DIT.

18. Software Support and Maintenance Services

The ideal solution will have established support and maintenance. Please explain the following regarding these services:

- a. Describe how the service desk operates; i.e., service hours, escalation of problems, ticket tracking, reporting of metrics on availability, call scripts, repository of solutions, call back time etc.
- b. Describe how the solution will provide availability and uptime metrics for solution.
- c. Describe the solution's development "sandbox" as envisioned for backend integration efforts with legacy environments.
- d. Describe how the application changes will be able to be previewed in a "sandbox"/non-production environment prior to changes being made in production.
- e. Describe the management and project team assigned to work with North Carolina.
- f. Describe the process for incident management, change management and release management.
- g. Provide a list and description of the required roles and level of staff resources to manage, monitor, maintain and support the overall solution.

19. Training

The State desires a solution that will employ training techniques with the capability to accommodate various levels of users. Training will be needed for each department/division/unit to include form modification, workflow creation/modifications, and assistance with onboarding users including signature creation. Describe the solution's training regarding:

- a. What modes of user training are available?
- b. What level of training comes with the proposal?
- c. What type of training will be provided in the proposal for the new use cases and purchases? (to include form modification, workflow creation/modifications, and assistance with on-boarding users including signature creation.)
- d. What online help capabilities are available for users?
- e. What online help capabilities are available for administrators?
- f. What web-based documentation is provided?

- g. What live and web-based technical support is provided?
- h. What types of training and documentation is provided for API usage?
- i. Describe the ability to provide cloud based user “sandbox” areas to support user on boarding, training, and functional trials. Specifically discuss limitations as related to function of the production system as well as trial or usage limits.
- j. Describe whether the proposed solution requires customer to procure or implement any additional, on-premise hardware or technology commodities for proposed solution to function. Specify requirements by including descriptions, manufacturers, and model numbers.
- k. Provide information regarding user communities and/or support groups.

IV. Cost Proposal

OFFER COSTS: The Vendor must list and describe any applicable offer costs which may include the following:

- 1) Vendor shall be able to accept individual and/or Agency Wide Purchases on behalf of the agency and count toward the tiered pricing of that Agency.
- 2) Can Transactions/licensing fees be billed by Department/Division/Unit?
- 3) Pricing based on total transaction volume for the State.
- 4) Explain usage and meaning of document, folder, and transaction system identifiers. Usage counts will need to correspond with Cost Proposal in **Section IV.**
- 5) Describe the purchase process for an Agency.
- 6) Define the minimum transaction purchase.
- 7) Define the Costs for Connectors to *SharePoint, Dynamics 365, Salesforce etc.*
 - a. What costs are there to integrate into SharePoint?, Azure, Amazon Webservices, Dynamics 365, and Salesforce.com.
 - b. What other CRM solutions or cloud solutions do you integrate with? Provide list and a cost for each.
- 8) Define what is included in the Named users, Tiered, and unlimited pricing models. Support, training, adoption etc..
- 9) Define Unlimited or Enterprise in terms of who can utilize this model.
- 10) Define what constitutes a transaction from a cost standpoint? Specifically, Voided Transactions and bulk Downloads.
- 11) Define Adoption accelerator costs if offered?
- 12) Define the service level, description and costs for Standard, Premium, and Dedicated Support?
- 13) Is Unlimited phone technical support available for users, power users and administrators?
- 14) Define what happens to the number of Transactions that are not used during the contract term and yearly anniversary.
- 15) Define the licensing model offered and how signatures and transactions are counted.

- 16) NCID Integration-This is a de-centralized model and each Agency will have its own solution; therefore, define the cost for integration. Consider
- a) Storage – How much storage is included with each cost model.
 - b) Exit Strategy – Define the cost for downloading transactions- Define how this process works
 - c) What is the cost for bulk retrieval of documents?
 - d) Migration costs from existing signature systems
 - e) Are there costs for Voided Transaction if any?
 - f) Is there customization required or proposed addressing specification. If so, what is the cost.
 - g) Are there additional modules required or proposed addressing specifications
 - h) Are there any installation/conversion/integration/transition costs?
 - i) Provide all training costs by type; user, admin, power user. What is included in each cost model.
 - j) Maintenance costs per year- Is this an evergreen product and updates are included?
 - k) Do you have a professional consulting service or other value added service based on hourly rates? Provide your hourly costs. Travel and lodging expenses, if any, must be thoroughly described; and are limited by the State's Terms and Conditions.

Item #	QTY	Unit	Description	Ext Cost
1.	1	User/year	Named User	
2.	5	Users/year	Named User	
3.	25	Users/year	Named User	
4.	100	Transaction/year	Package of signatures	
5.	500	Transaction/year	Package of signatures	
6.	2500	Transaction/year	Package of signatures	
7.	5000	Transaction/year	Package of signatures	
8.	10000	Transaction/year	Package of signatures	
9.	20000	Transaction/year	Package of signatures	
10.	50000	Transaction/year	Package of signatures	

Item #	QTY	Unit	Description	Ext Cost
11.	75000	Transaction/year	Package of signatures	
12.	100000	Transaction/year	Package of signatures	
13.	Unlimited	Transaction/year	Package of signatures	
14.	NA	NA	NCID integration	
15.	Storage	MB	Cost for Form Storage	
16.		Per Connector	Connector to Dynamics 365	
17.		Per Connector	Connector to Salesforce	
18.		Per Connector	Connector to SharePoint Online	
19.		Per Connector	Connector to SharePoint On Prem	
20.			Bulk retrieval of Transactions	
21.		Per hour?	Migration Costs	
22.	Vendor Define	Transaction/year	Costs for Voided Transactions	
23.	Vendor Define	Per hour	Professional Services	

17) **PAYMENT PLAN PROPOSAL:**

Vendors should note that multiple State agencies will leverage this contract, subsequently requiring the awarded vendor to invoice and provision each individual agency separately.

If Buying licenses/transactions in the middle of the term then they should be co-termed and prorated to the contract anniversary date.

- 18) **ALTERNATIVE COST RESPONSE:** Vendors who propose an Alternative cost response must submit a separate document labeled "ALTERNATIVE COST RESPONSE".

V. Other Requirements and Special Terms

- 1) **VENDOR UTILIZATION OF WORKERS OUTSIDE U.S.:** In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer. The Vendor shall provide the following for any offer or actual utilization or contract performance:
 - a) The location of work performed under a state contract by the Vendor, any subcontractors, employees, or other persons performing the Agreement and whether any of this work will be performed outside the United States
 - b) The corporate structure and location of corporate employees and activities of the Vendors, its affiliates or any other subcontractors
 - c) Notice of the relocation of the Vendor, employees of the Vendor, subcontractors of the Vendor, or other persons performing Services under a state contract outside of the United States
 - d) Any Vendor or subcontractor providing call or contact center Services to the State of North Carolina shall disclose to inbound callers the location from which the call or contact center Services are being provided

Will any work under the Agreement be performed outside the United States?

Where will Services be performed:

YES _____ NO _____

2) SPECIAL TERMS AND CONDITIONS:

- a) Paragraph #19 of the DIT Terms and Conditions is supplemented as follows: Any such audit shall be conducted only upon prior written notice of 30 days or more, and with the concurrence of The State for the date and time of any audit, and adherence to The State's security requirements during regular business hours at The State's offices and shall not unreasonably interfere with The State's business activities.
 - b) Paragraph #16 of the DIT Terms and Conditions is supplemented as follows: Each agency will be in their own instance and can successfully build and release signature transactions.
 - c) Reserved
 - d) Maintenance
- 3) **FINANCIAL STATEMENTS:** The Vendor shall provide evidence of financial stability with its response to this RFP as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.
- a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

- b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.
 - c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.
- 4) **DISCLOSURE OF LITIGATION:** Reserved.
 - 5) **CRIMINAL CONVICTION:** Reserved.
 - 6) **SECURITY AND BACKGROUND CHECKS:** Reserved.
 - 7) **ASSURANCES:** Reserved.
 - 8) **CONFIDENTIALITY OF DATA AND INFORMATION:** All RFP responses, information marked as confidential or proprietary, financial, statistical, personnel, technical and other data and information relating to the State's operation which are designated confidential by the State and made available to the Vendor in order to carry out the Agreement or which become available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to the State. If the methods and procedures employed by the Vendor for the protection of the Vendor's data and information are deemed by the State to be adequate for the protection of the State's confidential information, such methods and procedures may be used, with the written consent of the State, to carry out the intent of this section. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.
 - 9) **SOFTWARE TERMS:** Reserved.
 - 10) **PROJECT MANAGEMENT:** All coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of Vendor's work. All work

performed pursuant to the Agreement shall be coordinated between the Agency Project Manager and the Vendor's Project Manager.

- 11) **MEETINGS**: The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Agreement. Meetings will occur as problems arise and will be coordinated by Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations. Conference calls are should be sufficient as opposed to face-to-face meeting. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.
- 12) **STOP WORK ORDER**: The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.
 - a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
 - i) Cancel the Stop Work Order, or
 - ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.
 - b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
 - i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
 - ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.
 - c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable

direct costs resulting from the Stop Work Order in arriving at the termination settlement.

The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

- 13) **TRANSITION ASSISTANCE:** If this Agreement is not renewed at the end of this term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the State will be entitled to offset the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.
- 14) **TERM EXTENSIONS:** This agreement allows month-to-month or other term extensions at the discretion of the State.
- 15) **FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY:**
- a) Pursuant to N.C.G.S. §143B-1350(h)(1), Agencies must conduct a risk assessment, including whether the Vendor's has sufficient financial resources to satisfy the agreed upon limitation of liability prior to the award of a contract with Vendor.
 - b) Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.
 - c) Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.
- 16) **UNANTICIPATED TASKS:** Reserved.
- 17) **DUE DILIGENCE:** Reserved.
- 18) **AGENCY SITE VISITS:** Reserved.
- 19) **VENDOR SITE VISITS:** Reserved.
- 20) **RESELLERS:** If the Offer is made by a Reseller that purchased the offered items for resale or license to the Agency, or offered based upon an agreement between the Offeror and a third party, and that the proprietary and intellectual property rights associated with the items are owned by parties other than the Reseller ("Third Parties"). The Agency further acknowledges that except for the payment to the Reseller for the Third Party items, all of its rights and

obligations with respect thereto flow from and to the Third Parties. The Reseller shall provide the Agency with copies of all documentation and warranties for the Third Party items which are provided to the Reseller. The Reseller shall assign all applicable third party warranties for Deliverables to the Agency. The State reserves all rights to utilize existing agreements with such Third Parties or to negotiate agreements with such Third Parties as the State deems necessary or proper to achieve the intent of this RFP..

VI. Proposal Content and Organization

- 1) **CONTENTS OF PROPOSAL**: This section should contain all relevant and material information relating to the Vendor's organization, personnel, and experience that would substantiate its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If any relevant and material information is not provided, the offer may be rejected from consideration and evaluation. Offers will be considered and evaluated based upon the Vendor's full completion and response to the following, and any additional requirements herein, or stated in a separate Exhibit.
- 2) **INFORMATION AND DESCRIPTIVE LITERATURE**: The Vendor must furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with their offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these requirements may be rejected.
- 3) **PROPOSAL CONTENT**: Demonstrate substantial conformity to the RFP specifications.
 - a) Clearly state the understanding of the problem(s) presented by this RFP.
 - i) Response to technical specifications
 - ii) Cost offer
 - b) Detailed description of Vendor's firm should include all of the following:
 - i) Full name, address, and telephone number of the organization;
 - ii) Date established;
 - iii) Background of firm;
 - iv) Ownership (public company, partnership, subsidiary, etc.);
 - v) If incorporated, state of incorporation must be included.
 - vi) Number of full-time employees on January 1st for the last three years or for the duration that the Vendor's firm has been in business, whichever is less.
- 4) **ERRATA OR EXCEPTIONS**: Any errata or exceptions must be stated on a separate page, labeled "Errata and/or Exceptions" with references to the corresponding terms or provisions of the Solicitation.

- 5) **OFFER FORMAT:** The offers should contain the entire solicitation and be organized in the exact order in which the requirements and/or desirable performance criteria are presented in the RFP. **The Execution page of this RFP must be placed at the front of the Proposal.** Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP requirement and the specific page of the response in the Vendor's offer. All offers should be typewritten on standard 8 ½ x 11 paper (larger paper is permissible for charts, spreadsheets, etc.) and placed within a binder with tabs delineating each section.
- 6) **GENERAL INSTRUCTIONS:** Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:
- a) Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.
 - b) The response should be complete and comprehensive with a corresponding emphasis on being concise and clear.
- 7) **RFP RESPONSE ORGANIZATION:** The offer should be organized and indexed in the following format and should contain, at a minimum, all listed items in the sequence indicated.
- a) Letter of Transmittal - Each offer must be accompanied by a letter of transmittal that provides the following information:
 - i) Identify the submitting organization;
 - ii) Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized by the organization to contractually obligate the organization;
 - iii) Identify the name, title, telephone and fax number, along with an e-mail address of the person authorized to negotiate the Agreement on behalf of the organization;
 - iv) Identify the names, titles, telephone and fax number, along with an e-mail address of the person to be contacted for clarification;
 - v) Acknowledge receipt of any and all amendments to this RFP.
 - b) Table of Contents.
 - c) Response to Technical Specifications.
 - d) Completed Cost Offer.
 - e) References.
 - f) Financial Information.
 - g) Conflict of Interest:
 - i) Provide a statement that no assistance in preparing the response was received from any current or former employee of the State of North Carolina whose duties relate(d) to this RFP, unless such assistance was provided by the state employee in his or her official public capacity and that neither such employee nor any member of his or her immediate family has any financial interest in the outcome of this RFP;

- ii) State if the Vendor or any employee of the Vendor is related by blood or marriage to an Agency employee or resides with an Agency employee. If there are such relationships, list the names and relationships of said parties. Include the position and responsibilities within the Vendor's organization of such Vendor employees; and
 - iii) State the employing State Agency, individual's title at that State Agency, and termination date.
 - h) Errata and Exceptions, if any. Offers conditioned upon acceptance of Vendor Exceptions may be determined to be non-responsive by the State.
 - i) Copy of the Vendor's License and Maintenance Agreements, if any. The State reserves the right to edit or modify these agreements to conform to the best interest of the State.
 - j) Other Supporting Material Including Technical System Documentation.
 - k) Training and Other Materials, Samples or Examples.
 - l) Within each section of their offer, Vendors should address the items in the order in which they appear in this RFP. Forms, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of proposed costs, rates, or expenses must be presented with the cost response.
- 8) **ADHERENCE TO INSTRUCTIONS:** Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.
- 9) **ATTACHMENTS:** Vendors may attach other materials that they feel may improve the quality of their responses. However, these materials should be included as items in a separate appendix.

Attachment A. Department of Information Technology Terms and Conditions

1) DEFINITIONS:

- a) "Data" includes means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.
- b) Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.
- c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online services identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities.
- d) "State" shall mean the State of North Carolina, the Department of Information Technology as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.
- e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for users receiving similar Services.

2) ACCESS AND USE OF ONLINE SERVICES:

- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
- b) The State's right to access the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this right of access transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State

shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.

- c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's users for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.
 - d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
 - e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
 - f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
 - g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
 - h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT; REMEDIES.**
- a) Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become noninfringing. If neither of these options can

reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) **ACCESS AVAILABILITY; REMEDIES:**

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State. If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:
 - 1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
 - 2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
 - 3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the

Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10% service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) **EXCLUSIONS:**

- a) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- b) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.

6) **PERFORMANCE REVIEW AND ACCOUNTABILITY.** N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) **LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:**

- a) Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

8) **Vendor's Liability for Injury to Persons or Damage to Property:**

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Services either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.

- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or tangible personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of this Contract, whether tangible or intangible, arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
 - c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.
- 9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.
- 10) **TRANSITION PERIOD:**
- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
 - f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or

official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements with the Vendor. Violations of this provision may result in debarment of the Vendor(s) or Vendor(s) as permitted by 9 NCAC 06B.1207, or other provision of law.

14) **AVAILABILITY OF FUNDS:** Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the State for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the State's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement *is expressly contingent upon* the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the State will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to terminate any Services supplied to the State under this Agreement, and relieve the State of any further obligation thereof. The State shall remit payment for Services accepted on or prior to the date of the aforesaid notice in conformance with the payment terms.

15) **PAYMENT TERMS:**

- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein, but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
- b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
- c) For any third party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
- d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.

- e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

16) **ACCEPTANCE CRITERIA:**

- a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.
- b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld, but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

17) **CONFIDENTIALITY:** The State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1, *et seq.* Such information may include trade secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate information, Products, Services or appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL.**" By so marking any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions marked "confidential" meet the requirements of the Rules and Statutes set forth above. **However, under no circumstances shall price information be designated as confidential.** The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

18) **SECURITY OF STATE DATA:**

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it

by the State or maintained or created in accordance with this Agreement. No such information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data.. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i. The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii. That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii. That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security

liability insurance coverage for any loss resulting from a data breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;

- (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing

or other transmission of legally required notifications; (2) preparation and mailing or other transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. In the event that Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and also in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - 1) The scale and quantity of the State Data loss;
 - 2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - 3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - 4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n),

Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

- o) **Secure Data Disposal.** When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

19) **ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C. General Statute 147-64.7, the State, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Agreement. Additional audit or reporting requirements may be required by any State, if in the State's opinion, such requirement is imposed by federal or state law or regulation. The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.

20) **ASSIGNMENT:** Vendor may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days of any consolidation, acquisition, or merger. Any assignee shall affirm this Agreement attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

21) **NOTICES:** Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand.

22) **TITLES AND HEADINGS:** Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

23) **AMENDMENT:** This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.

24) **TAXES:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

25) **GOVERNING LAWS, JURISDICTION, AND VENUE:** This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

26) **DEFAULT:** In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the material requirements and specifications herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC

06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide Services as provided herein.
- b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.

27) **FORCE MAJEURE:** Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

28) **COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.

29) **TERMINATION:** Any notice or termination made under this Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated. The parties may mutually terminate this Agreement by written agreement at any time.

- a) The State may terminate this Agreement, in whole or in part, pursuant to the Paragraph entitled "Default," above, or pursuant to Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following
 - i) Termination for Cause: In the event any goods, Services, or service furnished by the Vendor during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 7), entitled "Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Services performed in conformance with the Agreement. In the event the Agreement is terminated for the convenience of the State the State will pay for all Services and work performed or delivered in conformance with the Agreement up to the date of termination.

30) **DISPUTE RESOLUTION:** The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

31) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

32) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the State shall be entitled to any and all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

33) **ELECTRONIC PROCUREMENT:** (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third-party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract. The E-Procurement fee does not normally apply to services.

- a) Reserved.
- b) Reserved.
- c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Agreement. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.
- d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

The following terms and conditions apply to Software as a Service (SaaS) solutions.

1) DEFINITIONS:

- a) "Data" includes means information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the Services pursuant to this Agreement. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

- b) Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State as included in Paragraph 7) c) of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.
 - c) "Services" shall mean the duties and tasks undertaken by the Vendor to fulfill the requirements and specifications of this solicitation, including, without limitation, providing web browser access by authorized users to certain Vendor online software applications identified herein, and to related services, such as Vendor hosted Computer storage, databases, Support, documentation, and other functionalities, all as a Software as a Service ("SaaS") solution.
 - d) "State" shall mean the State of North Carolina, the Department of Information Technology as an agency, or the agency identified in this solicitation as the Purchasing Agency and Award Authority.
 - e) "Support" includes provision of ongoing updates and maintenance for the Vendor online software applications, and as may be specified herein, consulting, training and other support Services as provided by the Vendor for SaaS tenants receiving similar SaaS Services.
- 2) **ACCESS AND USE OF SAAS SERVICES:**
- a) Vendor grants the State a personal non-transferable and non-exclusive right to use and access, all Services and other functionalities or services provided, furnished or accessible under this Agreement. The State may utilize the Services as agreed herein and in accordance with any mutually agreed Acceptable Use Policy. The State is authorized to access State Data and any Vendor-provided data as specified herein and to transmit revisions, updates, deletions, enhancements, or modifications to the State Data. This shall include the right of the State to, and access to, Support without the Vendor requiring a separate maintenance or support agreement. Subject to an agreed limitation on the number of users, the State may use the Services with any computer, computer system, server, or desktop workstation owned or utilized by the State or other authorized users. User access to the Services shall be routinely provided by the Vendor and may be subject to a more specific Service Level Agreement (SLA) agreed to in writing by the parties. The State shall notify the Vendor of any unauthorized use of any password or account, or any other known or suspected breach of security access. The State also agrees to refrain from taking any steps, such as reverse engineering, reverse assembly or reverse compilation to derive a source code equivalent to the Services or any portion thereof. Use of the Services to perform services for commercial third parties (so-called "service bureau" uses) is not permitted, but the State may utilize the Services to perform its governmental functions. If the Services fees are based upon the number of Users and/or hosted instances, the number of Users/hosted instances available may be adjusted at any time (subject to the restrictions on the maximum number of Users specified in the Furnish and Deliver Table herein above) by mutual agreement and State Procurement approval. All Services and information designated as "confidential" or "proprietary" shall be kept in confidence except as may be required by the North Carolina Public Records Act: N.C.G.S. § 132-1, *et. seq.*
 - b) The State's access license for the Services and its associated services neither transfers, vests, nor infers any title or other ownership right in any intellectual property rights of the Vendor or any third party, nor does this license transfer, vest, or infer any title or other ownership right in any source code associated with the Services unless otherwise agreed to by the parties. The provisions of this paragraph will not be construed as a sale of any ownership rights in the Services. Any Services or technical and business information owned by Vendor or its suppliers or licensors made accessible or furnished to the State shall be and remain the property of the Vendor or such other party, respectively. Vendor has a limited, non-exclusive license to access and use the State Data as provided to Vendor, but solely for performing its obligations under this Agreement and in confidence as provided herein.
 - c) Vendor or its suppliers shall at minimum, and except as otherwise agreed, provide telephone assistance to the State for all Services procured hereunder during the State's normal business hours (unless different hours are specified herein). Vendor warrants that

its Support and customer service and assistance will be performed in accordance with generally accepted industry standards. The State has the right to receive the benefit of upgrades, updates, maintenance releases or other enhancements or modifications made generally available to Vendor's SaaS tenants for similar Services. Vendor's right to a new use agreement for new version releases of the Services shall not be abridged by the foregoing. Vendor may, at no additional charge, modify the Services to improve operation and reliability or to meet legal requirements.

- d) Vendor will provide to the State the same Services for updating, maintaining and continuing optimal performance for the Services as provided to other similarly situated users or tenants of the Services, but minimally as provided for and specified herein. Unless otherwise agreed in writing, Support will also be provided for any other (e.g., third-party) software provided by the Vendor in connection with the Vendor's solution herein. The technical and professional activities required for establishing, managing, and maintaining the Services environment are the responsibilities of the Vendor. Any training specified herein will be provided by the Vendor to certain State users for the fees or costs as set forth herein or in an SLA.
 - e) Services provided pursuant to this Solicitation may, in some circumstances, be accompanied by a user clickwrap agreement. The term clickwrap agreement refers to an agreement that requires the end user to manifest his or her assent to terms and conditions by clicking an "ok" or "agree" button on a dialog box or pop-up window as part of the process of access to the Services. All terms and conditions of any clickwrap agreement provided with any Services solicited herein shall have no force and effect and shall be non-binding on the State, its employees, agents, and other authorized users of the Services.
 - f) The Vendor may utilize partners and/or subcontractors to assist in the provision of the Services, so long as the State Data is not removed from the United States unless the terms of storage of the State Data are clearly disclosed, the security provisions referenced herein can still be complied with, and such removal is done with the prior express written permission of the State. The Vendor shall identify all of its strategic business partners related to Services provided under this contract, including but not limited to, all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Vendor, who will be involved in any application development and/or operations.
 - g) Vendor warrants that all Services will be performed with professional care and skill, in a workmanlike manner and in accordance with the Services documentation and this Agreement.
 - h) An SLA or other agreed writing shall contain provisions for scalability of Services and any variation in fees or costs as a result of any such scaling.
 - i) Professional services provided by the Vendor at the request by the State in writing in addition to agreed Services shall be at the then-existing Vendor hourly rates when provided, unless otherwise agreed in writing by the parties.
- 3) **WARRANTY OF NON-INFRINGEMENT; REMEDIES.**
- a) Vendor warrants to the best of its knowledge that:
 - i) The Services do not infringe any intellectual property rights of any third party; and
 - ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
 - b) Should any Services supplied by Vendor become the subject of a claim of infringement of a patent, copyright, Trademark or a trade secret in the United States, the Vendor, shall at its option and expense, either procure for the State the right to continue using the Services, or replace or modify the same to become noninfringing. If neither of these options can reasonably be taken in Vendor's judgment, or if further use shall be prevented by injunction, the Vendor agrees to cease provision of any affected Services, and refund any sums the State has paid Vendor and make every reasonable effort to assist the State in procuring substitute Services. If, in the sole opinion of the State, the cessation of use by the State of any such Services due to infringement issues makes the retention of other items acquired from the Vendor under this Agreement impractical, the State shall then have the option of

terminating the Agreement, or applicable portions thereof, without penalty or termination charge; and Vendor agrees to refund any sums the State paid for unused Services.

- c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services supplied by the Vendor, their use or operation, infringes on a patent, copyright, trademark or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded or agreed in a settlement against the State in any such action. Such defense and payment shall be conditioned on the following:
 - i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
 - ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise provided, however, that the State shall have the option to participate in such action at its own expense.
- d) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation results from the State's material alteration of any Vendor-branded Services, or from the continued use of the good(s) or Services after receiving notice they infringe on a trade secret of a third party.

4) **ACCESS AVAILABILITY; REMEDIES:**

- a) The Vendor warrants that the Services will be in good working order, and operating in conformance with Vendor's standard specifications and functions as well as any other specifications agreed to by the parties in writing, and shall remain accessible 24/7, with the exception of scheduled outages for maintenance and of other service level provisions agreed in writing, e.g., in an SLA. Vendor does not warrant that the operation of the Services will be completely uninterrupted or error free, or that the Services functions will meet all the State's requirements, unless developed as Customized Services.
- b) The State shall notify the Vendor if the Services are not in good working order or inaccessible during the term of the Agreement. Vendor shall, at its option, either repair, replace or reperform any Services reported or discovered as not being in good working order and accessible during the applicable contract term without cost to the State. If the Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to receive automatic credits as indicated immediately below, or the State may use other contractual remedies such as recovery of damages, as set forth herein in writing, e.g., in Specifications, Special Terms or in an SLA, and as such other contractual damages are limited by N.C.G.S. §143B-1350(h1) and the Limitation of Liability paragraph below. If not otherwise provided, the automatic remedies for nonavailability of the Subscription Services during a month are:
 - 1. A 10% service credit applied against future fees if Vendor does not reach 99.9% availability.
 - 2. A 25% service credit applied against future fees if Vendor does not reach 99% availability.
 - 3. A 50% service credit applied against future fees or eligibility for early termination of the Agreement if Vendor does not reach 95% availability.

If, however, Services meet the 99.9% service availability level for a month, but are not available for a consecutive 120 minutes during that month, the Vendor shall grant to the State a credit of a pro-rated one-day of the monthly subscription Services fee against future Services charges. Such credit(s) shall be applied to the bill immediately following the month in which Vendor failed to meet the performance requirements or other service levels, and the credit will continue to be deducted from the monthly invoice for each prior month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement. If Services monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may also terminate the contract for material breach in accordance with the Default provisions hereinbelow.

- c) Support Services. If Vendor fails to meet Support Service response times as set forth herein or in an SLA for a period of three consecutive months, a 10% service credit will be deducted from the invoice in the month immediately following the third month, and the 10%

service credit will continue to be deducted from the monthly invoice for each month that Vendor fails to meet the support response times for the remainder of the duration of the Agreement.

5) **EXCLUSIONS:**

- c) Except as stated above in Paragraphs 3 and 4, Vendor and its parent, subsidiaries and affiliates, subcontractors and suppliers make no warranties, express or implied, as to the Services.
- d) The warranties provided in Paragraphs 3 and 4 above do not cover repair for damages, malfunctions or service failures substantially caused by:
 - i) Actions of non-Vendor personnel;
 - ii) Failure to follow Vendor's written instructions relating to the Services provided to the State; or
 - iii) Force Majeure conditions set forth hereinbelow.
 - iv) The State's sole misuse of, or its own inability to use, the Services.

6) **PERFORMANCE REVIEW AND ACCOUNTABILITY.** N.C.G.S. § 143B-1340(f) and 09 NCAC 06B.1207 require provisions for performance review and accountability in State IT contracts. For this procurement, these shall include the holding a retainage of 10% of the contract value and withholding the final payment contingent on final acceptance by the State as provided in 09 NCAC 06B.1207(3) and (4), unless waived or otherwise agreed, in writing. The Services herein will be provided consistent with and under these Services performance review and accountability guarantees.

7) **LIMITATION OF LIABILITY: Limitation of Vendor's Contract Damages Liability:**

- a) Where Services are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Services and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Services.
- b) The Vendor's liability for damages to the State arising under the contract shall be limited to two times the value of the Contract.
- c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranty compliance, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 et seq., the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on this Contract. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

8) **Vendor's Liability for Injury to Persons or Damage to Property:**

- a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Services either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.
- b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or tangible personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of this Contract, whether tangible or intangible,

- arising out of the ordinary negligence, willful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.
- c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.
- 9) **MODIFICATION OF SERVICES:** If Vendor modifies or replaces the Services provided to the State and other tenants, and if the State has paid all applicable Subscription Fees, the State shall be entitled to receive, at no additional charge, access to a newer version of the Services that supports substantially the same functionality as the then accessible version of the Services. Newer versions of the Services containing substantially increased functionality may be made available to the State for an additional subscription fee. In the event of either of such modifications, the then accessible version of the Services shall remain fully available to the State until the newer version is provided to the State and accepted. If a modification materially affects the functionality of the Services as used by the State, the State, at its sole option, may defer such modification.
- 10) **TRANSITION PERIOD:**
- a) For ninety (90) days, either prior to the expiration date of this Agreement, or upon notice of termination of this Agreement, Vendor shall assist the State, upon written request, in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
 - b) The Transition Period may be modified in an SLA or as agreed upon in writing by the parties in a contract amendment.
 - c) During the Transition Period, Services access shall continue to be made available to the State without alteration.
 - d) Vendor agrees to compensate the State for damages or losses the State incurs as a result of Vendor's failure to comply with this Transition Period section in accordance with the Limitation of Liability provisions above.
 - e) Upon termination, and unless otherwise stated in an SLA, and after providing the State Data to the State as indicated above in this section with acknowledged receipt by the State in writing, the Vendor shall permanently destroy or render inaccessible any portion of the State Data in Vendor's and/or subcontractor's possession or control following the completion and expiration of all obligations in this section. Within thirty (30) days, Vendor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
 - f) The State at its option, may purchase additional Transition services as may be agreed upon in a supplemental agreement.
- 11) **TRANSPORTATION:** Transportation charges for any Deliverable sent to the State other than electronically or by download, shall be FOB Destination unless delivered by internet or file-transfer as agreed by the State, or otherwise specified in the solicitation document or purchase order.
- 12) **TRAVEL EXPENSES:** All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed. In the event that the Vendor may be eligible to be reimbursed for travel expenses specifically agreed to in writing and arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under this Agreement.
- 13) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any contract or award issued by the State. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding Agreements with the Vendor.

Violations of this provision may result in debarment of the Vendor(s) or Vendor(s) as permitted by 9 NCAC 06B.1207, or other provision of law.

- 14) **AVAILABILITY OF FUNDS:** Any and all payments by the State are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the State for the purposes set forth in this Agreement. If this Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the State's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of this Agreement extends into fiscal years subsequent to that in which it is approved such continuation of the Agreement *is expressly contingent upon* the appropriation, allocation, and availability of funds by the N.C. Legislature for the purposes set forth in the Agreement. If funds to effect payment are not available, the State will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to terminate any Services supplied to the State under this Agreement, and relieve the State of any further obligation thereof. The State shall remit payment for Services accepted on or prior to the date of the aforesaid notice in conformance with the payment terms.

15) **PAYMENT TERMS:**

- a) Payment may be made by the State in advance of or in anticipation of subscription Services to be actually performed under the Agreement or upon proper invoice for other Services rendered. Payment terms are Net 30 days after receipt of correct invoice. Initial payments are to be made after final acceptance of the Services. Payments are subject to any retainage requirements herein. The Purchasing State Agency is responsible for all payments under the Agreement. Subscription fees for term years after the initial year shall be as quoted under State options herein, but shall not increase more than 5% over the prior term, except as the parties may have agreed to an alternate formula to determine such increases in writing. No additional charges to the State will be permitted based upon, or arising from, the State's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et seq.* of the N.C. General Statutes and applicable Administrative Rules.
- b) Upon Vendor's written request of not less than 30 days and approval by the State, the State may:
 - i. Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
 - ii. Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however,
 - iii. In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Agreement obligations.
- c) For any third party software licensed by Vendor or its subcontractors for use by the State, a copy of the software license including terms acceptable to the State, an assignment acceptable to the State, and documentation of license fees paid by the Vendor must be provided to the State before any related license fees or costs may be billed to the State.
- d) An undisputed invoice is an invoice for which the State and/or the Purchasing State Agency has not disputed in writing within thirty (30) days from the invoice date, unless the agency requests more time for review of the invoice. Upon Vendor's receipt of a disputed invoice notice, Vendor will work to correct the applicable invoice error, provided that such dispute notice shall not relieve the State or the applicable Purchasing State Agency from its payment obligations for the undisputed items on the invoice or for any disputed items that are ultimately corrected. The Purchasing State Agency is not required to pay the Vendor for any Software or Services provided without a written purchase order from the appropriate Purchasing State Agency. In addition, all such Services provided must meet all terms, conditions, and specifications of this Agreement and purchase order and be accepted as satisfactory by the Purchasing State Agency before payment will be issued.
- e) The Purchasing State Agency shall release any amounts held as retainages for Services completed within a reasonable period after the end of the period(s) or term(s) for which the retainage was withheld. Payment retainage shall apply to all invoiced items, excepting only

such items as Vendor obtains from Third Parties and for which costs are chargeable to the State by agreement of the Parties. The Purchasing State Agency, in its sole discretion, may release retainages withheld from any invoice upon acceptance of the Services identified or associated with such invoices.

16) ACCEPTANCE CRITERIA:

- a) Initial acceptance testing is required for all Vendor supplied Services before going live, unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications and Vendor's technical representations. Acceptance of Services may be controlled by additional written terms as agreed by the parties.
- b) After initial acceptance of Services, the State shall have the obligation to notify Vendor, in writing and within ten (10) days following provision of any Deliverable described in the contract if it is not acceptable. The notice shall specify in reasonable detail the reason(s) a Deliverable is unacceptable. Acceptance by the State of any Vendor re-performance or correction shall not be unreasonably withheld, but may be conditioned or delayed as required for confirmation by the State that the issue(s) in the notice have been successfully corrected.

- 17) CONFIDENTIALITY:** The State may maintain the confidentiality of certain types of information described in N.C. Gen. Stat. §132-1, *et seq.* Such information may include trade secrets defined by N.C. Gen. Stat. §66-152 and other information exempted from the Public Records Act pursuant to N.C. Gen. Stat. §132-1.2. Vendor may designate information, Products, Services or appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL.**" By so marking any page, or portion of a page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors, that the portions marked "confidential" meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. If an action is brought pursuant to N.C. Gen. Stat. §132-9 to compel the State to disclose information marked "confidential," the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C. Gen. Stat. §132-9 or other applicable law.

18) SECURITY OF STATE DATA:

- a) All materials, including software, Data, information and documentation provided by the State to the Vendor (State Data) during the performance or provision of Services hereunder are the property of the State of North Carolina and must be kept secure and returned to the State. The Vendor will protect State Data in its hands from unauthorized disclosure, loss, damage, destruction by natural event, or other eventuality. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be provided to the State as part of the Services. The Vendor shall not access State User accounts, or State Data, except (i) during data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State's written request. The Vendor shall protect the confidentiality of all information, Data, instruments, studies, reports, records and other materials provided to it by the State or maintained or created in accordance with this Agreement. No such

information, Data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written agreement with the State. The Vendor will have written policies governing access to and duplication and dissemination of all such information, Data, instruments, studies, reports, records and other materials.

- b) The Vendor shall not store or transfer non-public State data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of North Carolina data remotely only as required to provide technical support.
- c) Protection of personal privacy and sensitive data. The Vendor acknowledges its responsibility for securing any restricted or highly restricted data, as defined by the Statewide Data Classification and Handling Policy (<https://it.nc.gov/document/statewide-data-classification-and-handling-policy>) that is collected by the State and stored in any Vendor site or other Vendor housing systems including, but not limited to, computer systems, networks, servers, or databases, maintained by Vendor or its agents or subcontractors in connection with the provision of the Services. The Vendor warrants, at its sole cost and expense, that it shall implement processes and maintain the security of data classified as restricted or highly restricted; provide reasonable care and efforts to detect fraudulent activity involving the data; and promptly notify the State of any breaches of security within 24 hours of confirmation as required by N.C.G.S. § 143B-1379.
- d) The Vendor will provide and maintain secure backup of the State Data. The Vendor shall implement and maintain secure passwords for its online system providing the Services, as well as all appropriate administrative, physical, technical and procedural safeguards at all times during the term of this Agreement to secure such Data from Data Breach, protect the Data and the Services from loss, corruption, unauthorized disclosure, and the introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data and the Services. The Vendor will allow periodic back-up of State Data by the State to the State's infrastructure as the State requires or as may be provided by law.
- e) The Vendor shall certify to the State:
 - i. The sufficiency of its security standards, tools, technologies and procedures in providing Services under this Agreement;
 - ii. That the system used to provide the Subscription Services under this Contract has and will maintain a valid 3rd party security certification not to exceed 1 year and is consistent with the data classification level and a security controls appropriate for low or moderate information system(s) per the National Institute of Standards and Technology NIST 800-53 revision 4. The State reserves the right to independently evaluate, audit, and verify such requirements.
 - iii. That the Services will comply with the following:
 - (1) Any DIT security policy regarding Cloud Computing, and the DIT Statewide Information Security Policy Manual; to include encryption requirements as defined below:
 - (a) The Vendor shall encrypt all non-public data in transit regardless of the transit mechanism.
 - (b) For engagements where the Vendor stores sensitive personally identifiable or otherwise confidential information, this data shall be encrypted at rest. Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Vendor's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, it must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data

breach. Additionally, where encryption of data at rest is not possible, the Vendor must describe existing security measures that provide a similar level of protection;

- (2) Privacy provisions of the Federal Privacy Act of 1974;
 - (3) The North Carolina Identity Theft Protection Act, N.C.G.S. Chapter 75, Article 2A (e.g., N.C.G.S. § 75-65 and -66);
 - (4) The North Carolina Public Records Act, N.C.G.S. Chapter 132; and
 - (5) Applicable Federal, State and industry standards and guidelines including, but not limited to, relevant security provisions of the Payment Card Industry (PCI) Data Security Standard (PCIDSS) including the PCIDSS Cloud Computing Guidelines, Criminal Justice Information, The Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA);
 - (6) Any requirements implemented by the State under N.C.G.S. §§ 143B-1376 and -1377.
- f) Security Breach. "Security Breach" under the NC Identity Theft Protection Act (N.C.G.S. § 75-60ff) means (1) any circumstance pursuant to which applicable Law requires notification of such breach to be given to affected parties or other activity in response to such circumstance (e.g., N.C.G.S. § 75-65); or (2) any actual, attempted, suspected, threatened, or reasonably foreseeable circumstance that compromises, or could reasonably be expected to compromise, either Physical Security or Systems Security (as such terms are defined below) in a fashion that either does or could reasonably be expected to permit unauthorized Processing (as defined below), use, disclosure or acquisition of or access to any the State Data or state confidential information. "Physical Security" means physical security at any site or other location housing systems maintained by Vendor or its agents or subcontractors in connection with the Services. "Systems Security" means security of computer, electronic or telecommunications systems of any variety (including data bases, hardware, software, storage, switching and interconnection devices and mechanisms), and networks of which such systems are a part or communicate with, used directly or indirectly by Vendor or its agents or subcontractors in connection with the Services. "Processing" means any operation or set of operations performed upon the State Data or State confidential information, whether by automatic means, such as creating, collecting, procuring, obtaining, accessing, recording, organizing, storing, adapting, altering, retrieving, consulting, using, disclosing or destroying.
- g) Breach Notification. In the event Vendor becomes aware of any Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall, at its own expense, (1) immediately notify the State's Agreement Administrator of such Security Breach and perform a root cause analysis thereon, (2) investigate such Security Breach, (3) provide a remediation plan, acceptable to the State, to address the Security Breach and prevent any further incidents, (4) conduct a forensic investigation to determine what systems, data and information have been affected by such event; and (5) cooperate with the State, and any law enforcement or regulatory officials, credit reporting companies, and credit card associations investigating such Security Breach. The State shall make the final decision on notifying the State's persons, entities, employees, service providers and/or the public of such Security Breach, and the implementation of the remediation plan. If a notification to a customer is required under any Law or pursuant to any of the State's privacy or security policies, then notifications to all persons and entities who are affected by the same event (as reasonably determined by the State) shall be considered legally required.
- h) Notification Related Costs. Vendor shall reimburse the State for all Notification Related Costs incurred by the State arising out of or in connection with any such Security Breach due to Vendor acts or omissions other than in accordance with the terms of the Agreement resulting in a requirement for legally required notifications. "Notification Related Costs" shall include the State's internal and external costs associated with addressing and responding to the Security Breach, including but not limited to: (1) preparation and mailing or other transmission of legally required notifications; (2) preparation and mailing or other

transmission of such other communications to customers, agents or others as the State deems reasonably appropriate; (3) establishment of a call center or other communications procedures in response to such Security Breach (e.g., customer service FAQs, talking points and training); (4) public relations and other similar crisis management services; (5) legal and accounting fees and expenses associated with the State's investigation of and response to such event; and (6) costs for credit reporting services that are associated with legally required notifications or are advisable, in the State's opinion, under the circumstances. If the Vendor becomes aware of any Security Breach which is not due to Vendor acts or omissions other than in accordance with the terms of the Agreement, Vendor shall immediately notify the State of such Security Breach, and the parties shall reasonably cooperate regarding which of the foregoing or other activities may be appropriate under the circumstances, including any applicable Charges for the same.

- i) Vendor shall allow the State reasonable access to Services security logs, latency statistics, and other related Services security data that affect this Agreement and the State's Data, at no cost to the State.
- j) In the course of normal operations, it may become necessary for Vendor to copy or move Data to another storage destination on its online system, and delete the Data found in the original location. In any such event, the Vendor shall preserve and maintain the content and integrity of the Data, except by prior written notice to, and prior written approval by, the State.
- k) Remote access to Data from outside the continental United States, including, without limitation, remote access to Data by authorized Services support staff in identified support centers, is prohibited unless approved in advance by the State Chief Information Officer or the Using Agency.
- l) In the event of temporary loss of access to Services, Vendor shall promptly restore continuity of Services, restore Data in accordance with this Agreement and as may be set forth in an SLA, restore accessibility of Data and the Services to meet the performance requirements stated herein or in an SLA. As a result, Service Level remedies will become available to the State as provided herein, in the SLA or other agreed and relevant documents. Failure to promptly remedy any such temporary loss of access may result in the State exercising its options for assessing damages under this Agreement.
- m) In the event of disaster or catastrophic failure that results in significant State Data loss or extended loss of access to Data or Services, Vendor shall notify the State by the fastest means available and in writing, with additional notification provided to the State Chief Information Officer or designee of the contracting agency. Vendor shall provide such notification within twenty-four (24) hours after Vendor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Vendor shall inform the State of:
 - 1) The scale and quantity of the State Data loss;
 - 2) What Vendor has done or will do to recover the State Data from backups and mitigate any deleterious effect of the State Data and Services loss; and
 - 3) What corrective action Vendor has taken or will take to prevent future State Data and Services loss.
 - 4) If Vendor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Agreement.

Vendor shall investigate of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Vendor shall cooperate fully with the State, its agents and law enforcement.

- n) In the event of termination of this contract, cessation of business by the Vendor or other event preventing Vendor from continuing to provide the Services, Vendor shall not withhold the State Data or any other State confidential information or refuse for any reason, to promptly return to the State the State Data and any other State confidential information (including copies thereof) if requested to do so on such media as reasonably requested by the State, even if the State is then or is alleged to be in breach of the Agreement. As a part of Vendor's obligation to provide the State Data pursuant to this Paragraph 18) n),

Vendor will also provide the State any data maps, documentation, software, or other materials necessary, including, without limitation, handwritten notes, materials, working papers or documentation, for the State to use, translate, interpret, extract and convert the State Data.

- o) **Secure Data Disposal.** When requested by the State, the Vendor shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.
- 19) **ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C. General Statute 147-64.7, the State, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of this Agreement or to costs charged to this Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of this Agreement. Additional audit or reporting requirements may be required by any State, if in the State's opinion, such requirement is imposed by federal or state law or regulation. The Vendor shall allow the State to audit conformance including contract terms, system security and data centers as appropriate. The State may perform this audit or contract with a third party at its discretion at the State's expense. Such reviews shall be conducted with at least 30 days' advance written notice and shall not unreasonably interfere with the Service Provider's business.
- 20) **ASSIGNMENT:** Vendor may not assign this Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days of any consolidation, acquisition, or merger. Any assignee shall affirm this Agreement attorning to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under this Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.
- 21) **NOTICES:** Any notices required under this Agreement should be delivered to the Agreement Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier, facsimile or by hand.
- 22) **TITLES AND HEADINGS:** Titles and Headings in this Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.
- 23) **AMENDMENT:** This Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor.
- 24) **TAXES:** The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of this Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.
- 25) **GOVERNING LAWS, JURISDICTION, AND VENUE:** This Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina. The place of this Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to this Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.
- 26) **DEFAULT:** In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the material requirements and specifications herein, the State may cancel the contract. Default may be cause for debarment as provided in

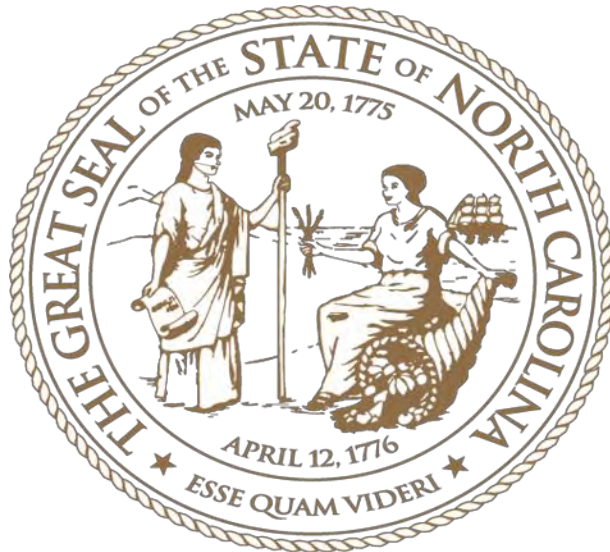
09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

- a) If Vendor fails to deliver or provide correct Services within the time required by this Contract, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide Services as provided herein.
 - b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such Vendor failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure. Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
- 27) **FORCE MAJEURE:** Except as provided for herein, neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.
- 28) **COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business and the provision of Services hereunder, including those of federal, state, and local agencies having jurisdiction and/or authority.
- 29) **TERMINATION:** Any notice or termination made under this Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated. The parties may mutually terminate this Agreement by written agreement at any time.
- a) The State may terminate this Agreement, in whole or in part, pursuant to the Paragraph entitled "Default," above, or pursuant to Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following
 - i) Termination for Cause: In the event any goods, Services, or service furnished by the Vendor during performance fails to conform to any material specification or requirement of the Agreement, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraph 7), entitled "Limitation of Liability." The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Agreement. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of this Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.
 - ii) Termination for Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Services performed in conformance with the Agreement. In the event the Agreement is terminated for the convenience of the State the State will pay for all Services and work performed or delivered in conformance with the Agreement up to the date of termination.

- 30) **DISPUTE RESOLUTION:** The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the State shall be submitted in writing to the Vendor's Agreement Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under this Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under this Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.
- 31) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of this Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of this Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.
- 32) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the State shall be entitled to any and all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.
- 33) **ELECTRONIC PROCUREMENT:** (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document): Purchasing shall be conducted through the Statewide E-Procurement Service. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Service. The Vendor shall register for the Statewide E-Procurement Service within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of this contract. The E-Procurement fee does not normally apply to services.
- a) Reserved.
 - b) Reserved.
 - c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Service. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Agreement. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, bids received, evaluation of bids received, award of contract, and the payment for goods delivered.
 - d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

**Attachment B. ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO) VENDOR ASSESSMENT
GUIDE**

**ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO)**



Vendor Readiness Assessment Report (VRR)

Executive Summary

The State requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Below is a high level view of specific security requirements that are requirements to meet compliance. Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates

Table of Contents

List of Tables

Table 3-1. System Information	4
Table 3-2. Leveraged Systems	4
Table 3-3. Leveraged Services	4
Table 3-3. System Interconnections	5
Table 3-4. Interconnection Security Agreements (ISAs)	5
Table 4-1. Federal Mandates	6
Table 4-2. Cryptographic Modules	7
Table 4-3. Transport Layer Security	7
Table 4-4. Identification and Authentication, Authorization, and Access Control	7
Table 4-5. Audit, Alerting, Malware, and Incident Response	8
Table 4-6. Contingency Planning and Disaster Recovery	9
Table 4-7. Configuration and Risk Management	10
Table 4-8. Data Center Security	11
Table 4-9. Policies and Procedures	12
Table 4-10. Missing Policy and Procedure Elements	13
Table 4-11. Security Awareness Training	14
Table 4-12. Staffing Levels	15
Table 4-13. Change Management	15
Table 4-14. Vendor Dependencies and Agreements	15
Table 4-15. Vendor Dependency Details	16
Table 4-16. Formal Agreements Details	16
Table 4-17. Continuous Monitoring Capabilities	16
Table 4-18. Continuous Monitoring Capabilities – Additional Details	16
Table 4-19. Maturity of the System Security Plan	17
Table 4-20. Controls Designated “Not Applicable”	17
Table 4-21. Controls with an Alternative Implementation	17

1. Introduction

○ Purpose

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific Cloud Service Provider's system based on organizational processes and the security capabilities of the Moderate/low-impact information system. The "**Outcome**" and the "**State Approach and Use of This Document**" sections below indicate how this document will impact this solicitation process.

○ Outcomes

Submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

○ State Approach and Use of This Document

The VRAR identifies clear and objective State security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the Vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities. Again, submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

Section 4, Capability Readiness, is organized into three sections:

- **Section 4.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. State **will not** waive any of these requirements.
- **Section 4.2, State Requirements**, identifies an excerpt of the most compelling requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. A VENDOR is unlikely to achieve approval if any of these requirements are not met.
- **Section 4.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a VENDOR's ability to achieve approval.

2. VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 3-1. System Information

VENDOR Name:
System Name:
Service Model: (IaaS, PaaS, SaaS)
FIPS PUB 199 System Security Level: (Moderate)
Fully Operational as of: Enter the date the system became fully operational.
Number of Customers (State/Others): Enter # of customers / # of other customers
Deployment Model: Is the service a Public Cloud, Government-Only Cloud, Federal Government-Only Cloud, or DOD Cloud?
System Functionality: Briefly describe the functionality of the system and service being provided.

Relationship to Other Vendors or CSPs

If this Moderate baseline system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 3-2 and 3-3 below. Please note, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note every capability in Section 4 that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

Table 3-2. Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?				If "yes," identify the underlying system.

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 3-2 above.

Table 3-3. Leveraged Services

#	Service	Service Capability	System
1	State what is being leveraged or "None" if no service is leveraged or if the VENDOR is responsible for the entire stack.	List the capability the service provides (e.g., load balancer, database, audit logging).	Identify the system from which the service is being leveraged.

Data Flow Diagrams

Insert Vendor-validated data flow diagram(s), and provide a written description of the data flows. The diagram(s) must:

- clearly identify anywhere State data is to be processed, stored, or transmitted;
- clearly delineate how data comes into and out of the system boundary;

- clearly identify data flows for privileged, non-privileged and customers access; and
- depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.

○ Separation Measures [AC-4, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

○ System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is “yes,” please briefly describe the connection. Also, if the answer to the last question is “yes,” please complete Table 3-4 below.

Table 3-3. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?			
2	Does the system connect to a corporate or state infrastructure/network?			
4	Does the system connect to external systems?			If “yes,” complete Table 3-4 below.

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type “None” in the first row.

Table 3-4. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1				
2				

3. Capability Readiness

○ State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 20, *State Requirements*, below.

Only answer “Yes” if the requirement is fully and strictly met. The Vendor must answer “No” if an alternative implementation is in place.

Table 4-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?		
2	What type of authentication does the application use? Can it integrate with the State's NCID solution?		
3	What types of security boundary/threat protection devices are used to protect the network, system, application...e.g. firewalls intrusion detection/prevention systems, end point protection etc.		
4	Does the VENDOR have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days?		
5	Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?		

○ State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

Approved Cryptographic Modules [SC-13]

The Vendor must ensure FIPS 140-2 **Validated** or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 **Compliant** is **not** sufficient. The Vendor may add rows to the table if appropriate, but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 4-2. Cryptographic Modules

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]						
2	Transmission [SC-8 (1), SC-12, SC-12(2, 3)]						
3	Remote Access [AC-17 (2)]						
4	Authentication [IA-5 (1), IA-7]						
5	Digital Signatures/Hash [CM-5 (3)]						

Transport Layer Security [NIST SP 800-52, Revision 1]

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 4-3. Transport Layer Security

#	The Cryptographic Module Type	Protocol In Use?		If “yes,” please describe use for both internal and external communications
		Yes	No	
1	SSL (Non-Compliant)			
2	TLS 1.0 (Non-Compliant)			
3	TLS 1.1 (Compliant)			
4	TLS 1.2 (Compliant)			

Identification and Authentication, Authorization, and Access Control

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)]			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)]			
4	Does the system fully comply with eAuth Level 3 or higher? [NIST SP 800-63]			<i>State the eAuth Level and provide sufficient details demonstrating that the system complies with this level, consistent with NIST SP 800-63.</i>
5	Does the system restrict non-authorized personnel's access to resources? [AC-6(2)]			
6	Does the system restrict non-privileged users from performing privileged function? [AC-6(10)]			
7	Does the system ensure secure separation of customer data? [SC-4]			
8	Does the system ensure secure separation of customer processing environments? [SC-2, SC-3]			<i>The capability description is not required here, but must be included in Section 3.3, Separation Measures.</i>
9	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)]			<i>The capability description is not required here, but must be included in Section 3.3, Separation Measures.</i>
10	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]			

Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)]			
2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-7, AU-9]			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-7, SI-7 (7)]			
4	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]			
5	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track and remediate security flaws? [SA-11, SA-11 (1), SA-11 (8)]			<i>If the system contains no custom software development, do not answer Y or N. Instead, state "NO CUSTOM CODE" here.</i>
6	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)]			
7	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-7, AU-7 (1), AU-11]			
8	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [State Incident Communications Procedures]			

Contingency Planning and Disaster Recovery

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10]			
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8]			

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]			
4	Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)]			
5	Does the system have backup power generation or other redundancy? [PE-11]			
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)]			

Configuration and Risk Management

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]			
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]			
3	Does the VENDOR have a Configuration Management Plan? [CM-9, CM-11]			
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4]			
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)]			
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)]			
•	• Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6]			<i>If “yes,” describe if the configuration settings are based on Center for Internet Security (CIS) Benchmarks or United States Government Configuration Baseline (USGCB), or “most restrictive consistent with operational requirements.”</i>

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]			

For the following questions, Vendors may use Table 4-18 “Continuous Monitoring Capabilities – Additional Details” to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5)]			<i>Describe how the Vendor validated that vulnerability scans were fully authenticated.</i>
10	Does the VENDOR demonstrate the capability to remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? [RA-5, State Continuous Monitoring policy]			<i>Describe how the Vendor validated that the VENDOR remediates High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days.</i>
11	When a High vulnerability is identified as part of ConMon activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5(8)]			

Data Center Security

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]			
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]			
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)]			

Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 4 families listed in Table 4-9 below.

To answer “yes” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each “-1” are fully addressed.

To answer “yes” to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 4-10 below.

Table 4-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]					Policy: • Procedure(s): •
2	Awareness & Training [AT-1]					Policy: • Procedure(s): •
3	Audit & Accountability [AU-1]					Policy: • Procedure(s): •
4	Security Assessment & Authorization [CA-1]					Policy: • Procedure(s): •
5	Configuration Management [CM-1]					Policy: • Procedure(s): •
6	Contingency Planning [CP-1]					Policy: • Procedure(s): •
7	Identification & Authentication [IA-1]					Policy: • Procedure(s): •

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
8	Incident Response [IR-1]					Policy: • Procedure(s): •
9	Maintenance [MA-1]					Policy: • Procedure(s): •
10	Media Protection [MP-1]					Policy: • Procedure(s): •
11	Physical & Environmental Protection [PE-1]					Policy: • Procedure(s): •
12	Personnel Security [PS-1]					Policy: • Procedure(s): •
13	Risk Assessment [RA-1]					Policy: • Procedure(s): •
14	System & Services Acquisition [SA-1]					Policy: • Procedure(s): •
15	System & Communications Protection [SC-1]					Policy: • Procedure(s): •
16	System & Information Integrity [SI-1]					Policy: • Procedure(s): •
17	Planning [PL-1]					Policy: • Procedure(s): •

For any family with a policy or procedure gap, please describe the gap below.

Table 4-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 4-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities?			

- **Additional Capability Information**

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

Staffing Levels

In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty.

Table 4-12. Staffing Levels

Staffing Levels

Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 4-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?			
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?			

Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 4-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?			<i>If "yes," please complete Table 4-15. Vendor Dependencies below.</i>
2	Within the system, are all products still actively supported by their respective vendors?			<i>If any are not supported, answer, "No."</i>
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?			<i>If "yes," please complete Table 4-16. Formal Agreements Details below.</i>

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Table 4-15. Vendor Dependency Details

#	Product and Vendor Name	Nature of Dependency	Still Supported?	
			Yes	No
1				
2				

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.

Table 4-16. Formal Agreements Details

#	Organization Name	Nature of Agreement
1		
2		

Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 4-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?			
2	Does the VENDOR have the ability to scan all hosts in the inventory?			
3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML, or .nessus files?			
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?			

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 4-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details

Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 4-19. Maturity of the System Security Plan

Maturity of the System Security Plan

In the table below, state the number of controls identified as “Not applicable” in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 4-20. Controls Designated “Not Applicable”

<x> Controls are Designated “Not Applicable”

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

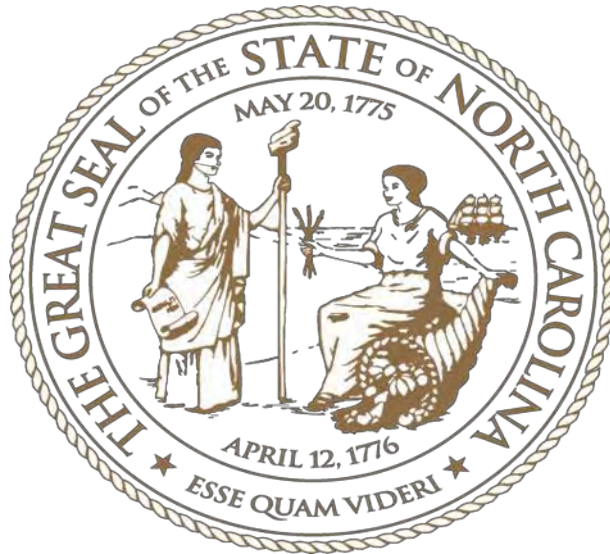
Table 4-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation

Appendix B: Completed Enterprise Security & Risk Management Office (ESRMO) Vendor Assessment Guide

**Attachment B. ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO) VENDOR ASSESSMENT
GUIDE**

**ENTERPRISE SECURITY & RISK
MANAGEMENT OFFICE (ESRMO)**



Vendor Readiness Assessment Report (VRR)

Executive Summary

The State requires that all systems connected to the State network or process State data, meet an acceptable level of security compliance. This includes those systems that operate outside of the States' direct control such as Cloud Services defined as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Below is a high level view of specific security requirements that are requirements to meet compliance. Note: There may be additional requirements depending on the sensitivity of the data and other Federal and State mandates

Table of Contents

List of Tables

Table 3-1. System Information	4
Table 3-2. Leveraged Systems	4
Table 3-3. Leveraged Services	4
Table 3-3. System Interconnections	5
Table 3-4. Interconnection Security Agreements (ISAs)	5
Table 4-1. Federal Mandates	6
Table 4-2. Cryptographic Modules	7
Table 4-3. Transport Layer Security	7
Table 4-4. Identification and Authentication, Authorization, and Access Control	7
Table 4-5. Audit, Alerting, Malware, and Incident Response	8
Table 4-6. Contingency Planning and Disaster Recovery	9
Table 4-7. Configuration and Risk Management	10
Table 4-8. Data Center Security	11
Table 4-9. Policies and Procedures	12
Table 4-10. Missing Policy and Procedure Elements	13
Table 4-11. Security Awareness Training	14
Table 4-12. Staffing Levels	15
Table 4-13. Change Management	15
Table 4-14. Vendor Dependencies and Agreements	15
Table 4-15. Vendor Dependency Details	16
Table 4-16. Formal Agreements Details	16
Table 4-17. Continuous Monitoring Capabilities	16
Table 4-18. Continuous Monitoring Capabilities – Additional Details	16
Table 4-19. Maturity of the System Security Plan	17
Table 4-20. Controls Designated “Not Applicable”	17
Table 4-21. Controls with an Alternative Implementation	17

1. Introduction

- **Purpose**

This report and its underlying assessment are intended to enable State agencies to reach a state-ready decision for a specific Cloud Service Provider's system based on organizational processes and the security capabilities of the Moderate/low-impact information system. The "**Outcome**" and the "**State Approach and Use of This Document**" sections below indicate how this document will impact this solicitation process.

- **Outcomes**

Submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

- **State Approach and Use of This Document**

The VRAR identifies clear and objective State security capability requirements, where possible, while also allowing for the presentation of more subjective information. The clear and objective requirements enable the Vendor to concisely identify whether an application or vendor is achieving the most important State Moderate or low baseline requirements. The combination of objective requirements and subjective information enables State to render a readiness decision based on a more complete understanding of the vendor's security capabilities. Again, submission of this report by the Vendor does not guarantee a state-ready designation, nor does it guarantee that the state will procure services from the vendor.

Section 4, Capability Readiness, is organized into three sections:

- **Section 4.1, State Mandates**, identifies a small set of the state mandates a vendor must satisfy. State **will not** waive any of these requirements.
- **Section 4.2, State Requirements**, identifies an excerpt of the most compelling requirements from the National Institute of Science and Technology (NIST) Special Publication (SP) 800 document series and State guidance. A VENDOR is unlikely to achieve approval if any of these requirements are not met.
- **Section 4.3, Additional Capability Information**, identifies additional information that is not tied to specific requirements, yet has typically reflected strongly on a VENDOR's ability to achieve approval.

2. VENDOR System Information

Provide and validate the information below. For example, if the deployment model is Government only, ensure there are no non-Government customers. The VRAR template is intended for systems categorized at the Moderate security impact level, in accordance with the FIPS Publication 199 Security Categorization.

Table 3-1. System Information

<p>VENDOR Name: Adobe Systems</p> <p>System Name: Adobe Sign</p> <p>Service Model: SaaS</p> <p>FIPS PUB 199 System Security Level: (Moderate)</p> <p>Fully Operational as of: July 18, 2011</p> <p>Number of Customers (State/Others): not disclosed</p> <p>Deployment Model: Public Cloud</p> <p>System Functionality: Briefly describe the functionality of the system and service being provided.</p>
--

Relationship to Other Vendors or CSPs

If this Moderate baseline system resides in another VENDOR's environment or inherits security capabilities, please provide the relevant details in Tables 3-2 and 3-3 below. Please note, the leveraged system itself must be State Authorized. For example, a large VENDOR may have a commercial service offering and a separate service offering with a State Authorization. Only the service offering with the State Authorization may be leveraged.

IMPORTANT: If there is a leveraged system, be sure to note every capability in Section 4 that partially or fully leverages the underlying system. When doing so, indicate the capability is fully inherited or describe both the inherited and non-inherited aspects of the capability.

Table 3-2. Leveraged Systems

#	Question	Yes	No	N/A	If Yes, please describe.
1	Is this system leveraging an underlying provider?	*			<p>Adobe Sign data centers are hosted by Amazon Web Services (AWS) and Microsoft Azure.</p> <ul style="list-style-type: none"> US geo is made up of 2 AWS locations, Virginia (NA1) and Oregon (NA2), both host primary/active and disaster recovery/passive instances of Adobe Sign as well as an Azure data center located in US-East (NA3 - active-only) EU geo is located in Frankfurt, Germany (primary/active) and Dublin, Ireland (disaster recovery/passive) Japan geo is located in Tokyo, JP (active-only)

					<ul style="list-style-type: none"> • Australia geo is located in Sydney, AU (active-only) • India geo is located in Mumbai, IN (active-only)
--	--	--	--	--	--

List all **services** leveraged. The system from which the service is leveraged must be listed in Table 3-2 above.

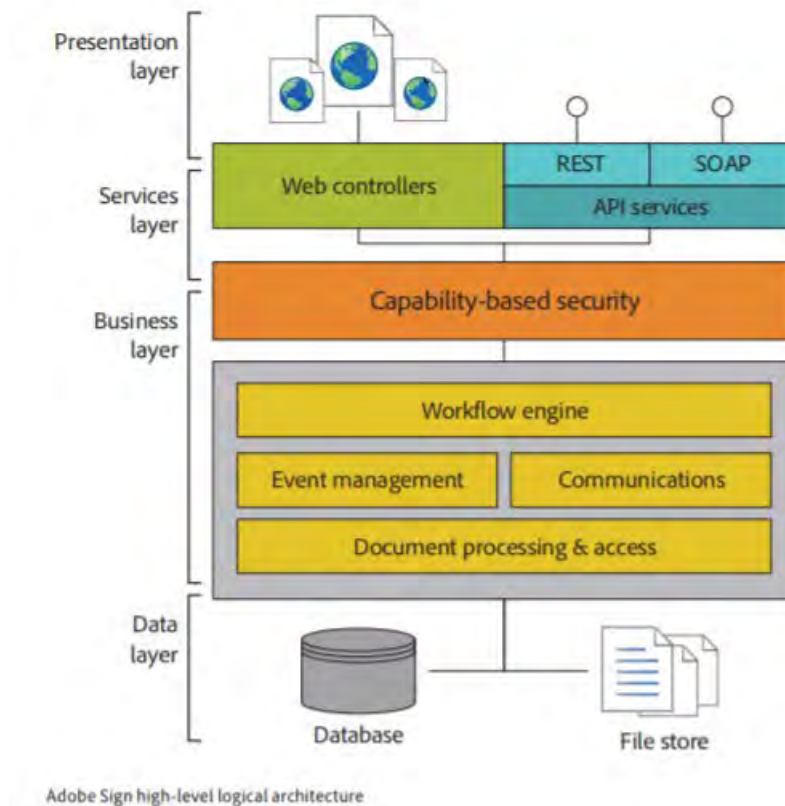
Table 3-3. Leveraged Services

#	Service	Service Capability	System
1	Hosting	Storage	AWS Datacenters

Data Flow Diagrams

Insert Vendor-validated data flow diagram(s), and provide a written description of the data flows. The diagram(s) must:

- clearly identify anywhere State data is to be processed, stored, or transmitted;
- clearly delineate how data comes into and out of the system boundary;



- clearly identify data flows for privileged, non-privileged and customers access; and
- depict how **all ports, protocols, and services** of all inbound and outbound traffic are represented and managed.

○ Separation Measures [AC-4, SC-7]

Assess and describe the strength of the physical and/or logical separation measures in place to provide segmentation and isolation of tenants, administration, and operations; addressing user-to-system; admin-to-system; and system-to-system relationships.

Document Cloud data stored by Adobe on AWS includes strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer, such as Document Cloud, from other AWS customers. AWS IAM is used to further lock down access to compute and storage instances. Please see <https://aws.amazon.com/security/> for more on AWS security.

The Vendor must base the assessment of separation measures on very strong evidence, such as the review of any existing penetration testing results, or an expert review of the products, architecture, and configurations involved. The Vendor must describe how the methods used to verify the strength of separation measures.

Please see <https://aws.amazon.com/security/> for more on AWS security.

○ System Interconnections

A System Interconnection is a dedicated connection between information systems, such as between a SaaS/PaaS and underlying IaaS.

The Vendor must complete the table below. If the answer to any question is “yes,” please briefly describe the connection. Also, if the answer to the last question is “yes,” please complete Table 3-4 below.

Table 3-3. System Interconnections

#	Question	Yes	No	If Yes, please describe.
1	Does the system connect to the Internet?	*		
2	Does the system connect to a corporate or state infrastructure/network?		*	
4	Does the system connect to external systems?		*	If “yes,” complete Table 3-4 below.

If there are connections to external systems, please list each in the table below, using one row per interconnection. If there are no external system connections, please type “None” in the first row.

Table 3-4. Interconnection Security Agreements (ISAs)

#	External System Connection	Does an ISA Exist?		Interconnection Description. If no ISA, please justify below.
		Yes	No	
1				
2				

3. Capability Readiness

○ State Mandates

This section identifies State requirements applicable to all State approved systems. All requirements in this section must be met. Some of these topics are also covered in greater detail in Section 4, *State Requirements*, below.

Only answer "Yes" if the requirement is fully and strictly met. The Vendor must answer "No" if an alternative implementation is in place.

Table 4-1. State Mandates

#	Compliance Topic	Fully Compliant?	
		Yes	No
1	Are FIPS 140-2 Validated or National Security Agency (NSA)-Approved cryptographic modules consistently used where cryptography is required?	*	
2	What type of authentication does the application use? Can it integrate with the State's NCID solution?	*	
3	What types of security boundary/threat protection devices are used to protect the network, system, application...e.g. firewalls intrusion detection/prevention systems, end point protection etc.	*	
4	Does the VENDOR have the ability to consistently remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days?	*	
5	Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?		*

○ State Requirements

This section identifies additional State Readiness requirements. All requirements in this section must be met; however, alternative implementations and non-applicability justifications may be considered on a limited basis.

Approved Cryptographic Modules [SC-13]

The Vendor must ensure FIPS 140-2 **Validated** or NSA-Approved algorithms are used for all encryption modules. FIPS 140-2 **Compliant** is **not** sufficient. The Vendor may add rows to the table if appropriate, but must not remove the original rows. The Vendor must identify all non-compliant cryptographic modules in use.

Table 4-2. Cryptographic Modules

	Cryptographic Module Type	FIPS 140-2 Validated?		NSA Approved?		Describe Any Alternative Implementations (if applicable)	Describe Missing Elements or N/A Justification
		Yes	No	Yes	No		
1	Data at Rest [SC-28]		*	*		Must use AWS Government Cloud	
2	Transmission [SC-8 (1), SC-12, SC-12(2, 3)]		*	*		Must use AWS Government Cloud	
3	Remote Access [AC-17 (2)]		*	*			
4	Authentication [IA-5 (1), IA-7]		*	*		SSO is available	
5	Digital Signatures/Hash [CM-5 (3)]	*		*			

Transport Layer Security [NIST SP 800-52, Revision 1]

The Vendor must identify all protocols in use. The Vendor may add rows to the table if appropriate, but must not remove the original rows.

Table 4-3. Transport Layer Security

#	The Cryptographic Module Type	Protocol In Use?		If “yes,” please describe use for both internal and external communications
		Yes	No	
1	SSL (Non-Compliant)		*	
2	TLS 1.0 (Non-Compliant)		*	
3	TLS 1.1 (Compliant)	*		All connections to Document Cloud are via HTTPS TLS (currently v1.1 or higher).
4	TLS 1.2 (Compliant)	*		All connections to Document Cloud are via HTTPS TLS (currently v1.1 or higher).

Identification and Authentication, Authorization, and Access Control

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-4. Identification and Authentication, Authorization, and Access Control

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
2	Does the system uniquely identify and authorize organizational users (or processes acting on behalf of organizational users) in a manner that cannot be repudiated and which sufficiently reduces the risk of impersonation? [IA-2, IA-4, IA-4(4)]	*		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system require multi-factor authentication (MFA) for administrative accounts and functions? [IA-2, IA-2(1), IA-2(3)]		*	Adobe has several types of accounts available to Enterprise customers, https://helpx.adobe.com/enterprise/help/identity.html . Allowing an IT Admin to require an account have 2FA enabled for both Adobe ID and Enterprise ID is not currently available but is on the roadmap. Adobe suggests enterprise customers who are interested in using two-factor authentication, use a Federated ID as it is created and owned by them, and that they work with an identity provider to set up two-factor authentication
4	Does the system fully comply with eAuth Level 3 or higher? [NIST SP 800-63]	*		eAuth Level 3 mandates multi factor authentication, this functionality is available but not the default.
5	Does the system restrict non-authorized personnel's access to resources? [AC-6(2)]	*		
6	Does the system restrict non-privileged users from performing privileged function? [AC-6(10)]	*		
7	Does the system ensure secure separation of customer data? [SC-4]	*		
8	Does the system ensure secure separation of customer processing environments? [SC-2, SC-3]	*		
9	Does the system restrict access of administrative personnel in a way that limits the capability of individuals to compromise the security of the information system? [AC-2(7)]	*		
10	Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure? [AC-17]		*	n/a

Audit, Alerting, Malware, and Incident Response

Only answer "yes" if the answer is consistently "yes." For partially implemented areas, answer "no" and describe what is missing to achieve a "yes" answer. If inherited, please indicate partial or full inheritance in the "Describe Capability" column. Any non-inherited capabilities must be described.

Table 4-5. Audit, Alerting, Malware, and Incident Response

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the system have the capability to detect, contain, and eradicate malicious software? [SI-3, SI-3 (1), SI-3 (2), SI-3 (7), MA-3 (2)]	*		

2	Does the system store audit data in a tamper-resistant manner which meets chain of custody and any e-discovery requirements? [AU-7, AU-9]	*		
---	---	---	--	--

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the VENDOR have the capability to detect unauthorized or malicious use of the system, including insider threat and external intrusions? [SI-4, SI-4 (4), SI-7, SI-7 (7)]	*		
4	Does the VENDOR have an Incident Response Plan and a fully developed Incident Response test plan? [IR-3, IR-8]	*		
5	Does the VENDOR have a plan and capability to perform security code analysis and assess code for security flaws, as well as identify, track and remediate security flaws? [SA-11, SA-11 (1), SA-11 (8)]	*		
6	Does the VENDOR implement automated mechanisms for incident handling and reporting? [IR-4 (1), IR-6 (1)]	*		
7	Does the VENDOR retain online audit records for at least 90 days to provide support for after-the-fact investigations of security incidents and offline for at least one year to meet regulatory and organizational information retention requirements? [AU-7, AU-7 (1), AU-11]	*		
8	Does the VENDOR have the capability to notify customers and regulators of confirmed incidents in a timeframe consistent with all legal, regulatory, or contractual obligations? [State Incident Communications Procedures]	*		

Contingency Planning and Disaster Recovery

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-6. Contingency Planning and Disaster Recovery

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have the capability to recover the system to a known and functional state following an outage, breach, DoS attack, or disaster? [CP-2, CP-2 (2), CP-2 (3), CP-9, CP-10]	*		
2	Does the VENDOR have a Contingency Plan and a fully developed Contingency Plan test plan in accordance with NIST Special Publication 800-34? [CP-2, CP-8]	*		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
3	Does the system have alternate storage and processing facilities? [CP-6, CP-7]	*		
4	Does the system have or use alternate telecommunications providers? [CP-8, CP-8 (2)]	*		
5	Does the system have backup power generation or other redundancy? [PE-11]	*		
6	Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers? [CP-8 (1)]		*	n/a . Adobe does not use telecommunication providers.

Configuration and Risk Management

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-7. Configuration and Risk Management

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR maintain a current, complete, and accurate baseline configuration of the information system? [CM-2]	*		
2	Does the VENDOR maintain a current, complete, and accurate inventory of the information system software, hardware, and network components? [CM-8]	*		
3	Does the VENDOR have a Configuration Management Plan? [CM-9, CM-11]	*		
4	Does the VENDOR follow a formal change control process that includes a security impact assessment? [CM-3, CM-4]	*		
5	Does the VENDOR employ automated mechanisms to detect inventory and configuration changes? [CM-2(2), CM-6(1), CM-8(3)]	*		
6	Does the VENDOR prevent unauthorized changes to the system? [CM-5, CM-5(1), CM-5(5)]	*		
•	• Does the VENDOR establish configuration settings for products employed that reflect the most restrictive mode consistent with operational requirements? [CM-6]	*		

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
8	Does the VENDOR ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP)-validated or SCAP-compatible (if validated checklists are not available)? [CM-6]	*		

For the following questions, Vendors may use Table 4-18 “Continuous Monitoring Capabilities – Additional Details” to enter the capability descriptions, supporting evidence, and missing elements.

9	Does the VENDOR perform authenticated operating system/ infrastructure, web, and database vulnerability scans at least monthly, as applicable? [RA-5, RA-5(5)]	*		For Document Cloud for enterprise, external scans are run on publicly facing IP addresses at least quarterly and after a significant product change. Internal vulnerability assessment scans must be conducted at least annually and after a significant change (code or feature change, or new release). In addition, vulnerability scans may occur as needed or when requested by teams or services. For all clouds, results are logged and tracked via an internal ticketing system. When vulnerabilities are reported to the Product Security Incident Response Team (PSIRT) team, they are logged, assigned and tracked via an internal ticketing system, as well.
10	Does the VENDOR demonstrate the capability to remediate High vulnerabilities within 30 days and Moderate vulnerabilities within 90 days? [RA-5, <i>State Continuous Monitoring policy</i>]	*		
11	When a High vulnerability is identified as part of Common activities, does the VENDOR consistently check audit logs for evidence of exploitation? [RA-5(8)]	*		

Data Center Security

Only answer “yes” if the answer is consistently “yes.” For partially implemented areas, answer “no” and describe what is missing to achieve a “yes” answer. If inherited, please indicate partial or full inheritance in the “Describe Capability” column. Any non-inherited capabilities must be described.

Table 4-8. Data Center Security

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR restrict physical system access to only authorized personnel? [PE-2 through PE-6, PE-8]	*		
2	Does the VENDOR monitor and log physical access to the information system, and maintain access records? [PE-6, PE-8]	*		
3	Does the VENDOR monitor and respond to physical intrusion alarms and surveillance equipment? [PE-6 (1)]	*		

Policies, Procedures, and Training

The Vendor must indicate the status of policy and procedure coverage for the NIST 800-53 Rev 4 families listed in Table 4-9 below.

To answer “yes” to a policy, it must be fully developed, documented, and disseminated; and it must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. A single policy document may address more than one family provided the NIST requirements of each “-1” are fully addressed.

To answer “yes” to a procedure, it must be fully developed and consistently followed by the appropriate staff. List all applicable procedure documents for each family.

VENDORS must establish their own set of Policies and Procedures (P&Ps). They cannot be inherited from a leveraged system, nor can they be provided by the customer. Any exceptions and/or missing policy and procedure elements must be explained in Table 4-10 below.

Table 4-9. Policies and Procedures

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
1	Access Control [AC-1]	*		*		Logical Account Access Standard. Version 3. Last modified November 2017.
2	Awareness & Training [AT-1]	*		*		Security Awareness Training Standard. Version 3. Last modified September 2017.
3	Audit & Accountability [AU-1]	*		*		Information Security Management Standard. Version 3. July 2017
4	Security Assessment & Authorization [CA-1]	*		*		Information Security Management Standard. Version 3. July 2017
5	Configuration Management [CM-1]	*		*		Change Management Standard. Version 3. November 2017.
6	Contingency Planning [CP-1]	*		*		Business Continuity Policy. Version 2. September 2017 Disaster Recovery Standard. Version 2. September 2017
7	Identification & Authentication [IA-1]	*		*		Authentication Standard. Version 3. August 2017

#	Family	Policy		Procedure		Title Version and Date
		Yes	No	Yes	No	
8	Incident Response [IR-1]	*		*		Computer Security Incident Response Standard. Version 3. September 2017
9	Maintenance [MA-1]	*		*		Employee-Assigned Asste Standard. Version 4.1. March 2018
10	Media Protection [MP-1]	*		*		Information Security Management Standard. Version 3. July 2017
11	Physical & Environmental Protection [PE-1]	*		*		Physical Security Policy. Version 5.0. February 2017
12	Personnel Security [PS-1]	*		*		Physical Security Policy. Version 5.0. February 2017
13	Risk Assessment [RA-1]	*		*		Risk Management Standard. Version 3. February 2018
14	System & Services Acquisition [SA-1]	*		*		Information Systems Asset Inventory Standard. Version 3. February 2018.
15	System & Communications Protection [SC-1]	*		*		Electronic Communications Policy. Version 4. January 2017
16	System & Information Integrity [SI-1]	*		*		Change Management Standard. Version 3. November 2017.
17	Planning [PL-1]	*		*		Information Security Management Standard. Version 3. July 2017

For any family with a policy or procedure gap, please describe the gap below.

Table 4-10. Missing Policy and Procedure Elements

Missing Policy and Procedure Elements
•

The Vendor must answer the questions below.

Table 4-11. Security Awareness Training

Question	Yes	No	Describe capability, supporting evidence, and any missing elements
Does the VENDOR train personnel on security awareness and role-based security responsibilities?	*		

○ **Additional Capability Information**

State will evaluate the responses in this section on a case-by-case basis relative to a State-Ready designation decision.

Staffing Levels

In the table below, the Vendor must describe the VENDOR's organizational structure, staffing levels currently dedicated to the security of the system, as well as any planned changes to these staffing levels. This description must clearly indicate role and number of individuals as well as identify which staff is full-time dedicated, and which are performing their role as a collateral duty.

Table 4-12. Staffing Levels

Staffing Levels

Unfortunately, Adobe does not release this information as it is proprietary.

Change Management Maturity

While the following change management capabilities are not required, they indicate a more mature change management capability and may influence a State Readiness decision, especially for larger systems.

The Vendor must answer the questions below.

Table 4-13. Change Management

#	Question	Yes	No	If "no", please describe how this is accomplished.
1	Does the VENDOR's change management capability include a fully functioning Change Control Board (CCB)?	*		
2	Does the VENDOR have and use development and/or test environments to verify changes before implementing them in the production environment?	*		

Vendor Dependencies and Agreements

The Vendor must answer the questions below.

Table 4-14. Vendor Dependencies and Agreements

#	Question	Yes	No	Instructions
1	Does the system have any dependencies on other vendors such as a leveraged service offering, hypervisor and operating system patches, physical security and/or software and hardware support?	*		If "yes," please complete Table 4-15. Vendor Dependencies below.
2	Within the system, are all products still actively supported by their respective vendors?	*		If any are not supported, answer, "No."
3	Does the VENDOR have a formal agreement with a vendor, such as for maintenance of a leveraged service offering?	*		If "yes," please complete Table 4-16. Formal Agreements Details below.

If there are vendor dependencies, please list each in the table below, using one row per dependency. For example, if using another vendor's operating system, list the operating system, version, and vendor name in the first column, briefly indicate the VENDOR's reliance on that vendor for patches, and indicate whether the vendor still develops and issues patches for that product. If there are no vendor dependencies, please type "None" in the first row.

Table 4-15. Vendor Dependency Details

#	Product and Vendor Name	Nature of Dependency	Still Supported?	
			Yes	No
1	Amazon Web Services	Hosting	*	
2	Microsoft Azure	Hosting	*	

If there are formal vendor agreements in place, please list each in the table below, using one row per agreement. If there are no formal agreements, please type "None" in the first row.

Table 4-16. Formal Agreements Details

#	Organization Name	Nature of Agreement
1	Amazon Web Services	SLA
2	Microsoft Azure	SLA

Continuous Monitoring Capabilities

In the tables below, please describe the current state of the VENDOR's Continuous Monitoring capabilities, as well as the length of time the VENDOR has been performing Continuous Monitoring for this system.

Table 4-17. Continuous Monitoring Capabilities

#	Question	Yes	No	Describe capability, supporting evidence, and any missing elements
1	Does the VENDOR have a lifecycle management plan that ensures products are updated before they reach the end of their vendor support period?	*		At Adobe, we have a robust Secure Product Lifecycle (SPLC) Process that ensures products are updated before they reach the end of their vendor support period.
2	Does the VENDOR have the ability to scan all hosts in the inventory?	*		For Document Cloud external scans are run on publicly facing IP addresses at least quarterly and after a significant product change. Internal vulnerability assessment scans must be conducted at least annually and after a significant change (code or feature change, or new release). In addition, vulnerability scans may occur as needed or when requested by teams or services. For all clouds, results are logged and tracked via an internal ticketing system. When vulnerabilities are reported to the Product Security Incident Response Team (PSIRT) team, they are logged, assigned and tracked via an internal ticketing system, as well.

3	Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML, or .nessus files?	*		n/a. Adobe does not make scan files externally viewable.
4	Is the VENDOR properly maintaining their Plan of Actions and Milestones (POA&M), including timely, accurate, and complete information entries for new scan findings, vendor check-ins, and closure of POA&M items?	*		For Document Cloud and Creative Cloud for enterprise, external scans are run on publicly facing IP addresses at least quarterly and after a significant product change. Internal vulnerability assessment scans must be conducted at least annually and after a significant change (code or feature change, or new release). In addition, vulnerability scans may occur as needed or when requested by teams or services. For all clouds, results are logged and tracked via an internal ticketing system. When vulnerabilities are reported to the Product Security Incident Response Team (PSIRT) team, they are logged, assigned and tracked via an internal ticketing system, as well.

In the table below, provide any additional details the Vendor believes to be relevant to State's understanding of the VENDOR's Continuous Monitoring Capabilities. If the Vendor has no additional details, please state, "None."

Table 4-18. Continuous Monitoring Capabilities – Additional Details

Continuous Monitoring Capabilities – Additional Details

Status of System Security Plan (SSP)

In the table below, explicitly state whether the SSP is fully developed, partially developed, or non-existent. Identify any sections that the VENDOR has not yet developed.

Table 4-19. Maturity of the System Security Plan

Maturity of the System Security Plan
<i>Fully developed</i>

In the table below, state the number of controls identified as “Not applicable” in the SSP. List the Control Identifier for each, and indicate whether a justification for each has been provided in the SSP control statement.

Table 4-20. Controls Designated “Not Applicable”

<x> Controls are Designated “Not Applicable”	
Table 4-19. Maturity of the System Security Plan	
Control Identifier	Existing Justification
Does the VENDOR have the ability to provide scan files in a structure data format, such as CSV, XML, or .nessus files?	Yes
Does the VENDOR have service level agreements (SLAs) in place with all telecommunications providers?	Yes
Does the remote access capability include VENDOR-defined and implemented usage restrictions, configuration guidance, and authorization procedure?	No

In the table below, state the number of controls with an alternative implementation. List the Control Identifier for each.

Table 4-21. Controls with an Alternative Implementation

<x> Controls have an Alternative Implementation	
Table 4-19. Maturity of the System Security Plan	
Control Identifier	Existing Justification
Does the VENDOR and system meet Federal Records Management Requirements, including the ability to support record holds, National Archives and Records Administration (NARA) requirements, and Freedom of Information Act (FOIA) requirements?	Adobe does not support legal holds. A customer is responsible for any claims of spoilage. Adobe Reader does support archiving PDFs.

Appendix C:

Attachment C: Acknowledged Addenda



Solicitation Addendum

Solicitation Number: ITS-400335
Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability
Solicitation Opening Date and Time: July 12, 2018 @ 2:00pm
Addendum Number: 1
Addendum Date: June 11, 2018
Contract Specialist or Purchasing Agent: Kristen Burnette, Contract and Vendor Manager
Kristen.burnette@nc.gov 919-754-6678

-
1. This addendum does not need to be returned.
 2. Special instructions on Interactive Purchasing System (IPS) was corrected to show the following:
Enterprise Electronic Forms and Digital Signature Capability RFP
Written questions must be submitted by 2:00pm on June 21, 2018.

Execute Addendum:

Offeror: CDW GOVERNMENT LLC
Authorized Signature: Larissa D. Newman
Name and Titled (Typed): LARISSA D. NEWMAN, CAPTURE MANAGER
Date: July 19th, 2018



Solicitation Addendum

Solicitation Number: ITS-400335
Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability
Solicitation Opening Date and Time: July 24, 2018 @ 2:00pm
Addendum Number: 2
Addendum Date: July 9, 2018
Contract Specialist or Purchasing Agent: Kristen Burnette, Contract and Vendor Manager
Kristen.burnette@nc.gov 919-754-6678

-
1. This addendum does not need to be returned.
 2. The solicitation is hereby modified as follows:
 - M1. The RFP ITS-400335 Bid opening has been extended to: **July 24 at 2:00 PM EST.**

Execute Addendum:

Offeror: COW GOVERNMENT LLC
Authorized Signature: *Larissa O. Newman*
Name and Titled (Typed): LARISSA O. NEWMAN, CAPTURE MANAGER
Date: JULY 19th, 2018



Solicitation Addendum

Solicitation Number: ITS-400335

Solicitation Description: Enterprise Electronic Forms and Digital Signature Capability

Solicitation Opening Date and Time: July 24, 2018 @ 2:00pm

Addendum Number: 3

Addendum Date: July 11, 2018

Contract Specialist or Kristen Burnette, Contract and Vendor Manager

Purchasing Agent: Kristen.burnette@nc.gov 919-754-6678

1. Return one properly executed copy of this addendum with bid response prior to the Solicitation Opening Date and Time listed above.
2. **This solicitation is hereby modified to remove Section II, 6) Branding.**
3. Following are questions received about the solicitation and the State's answers to the questions.

Question #	Vendor Question	The State's Response
1	Please confirm that you will you consider two different solutions, one for enterprise electronic forms and one for digital signatures. Can we respond to the one solution we offer and disregard the items for the one we do not?	We are looking for a turnkey solution like we have today which allows for forms and Signature.
2	What electronic signature vendor are you replacing? Why? Cost? Functionality?	The purpose of this RFP is to establish a multi-vendor/ multi-solution statewide convenience contract. Our current solution is DocuSign which could be included on the new Statewide contract.
3	Will the state be open to accepting (Since SaaS offerings are multi-tenant) the T&C's of the vendor? Unless it is run in a private cloud, a public cloud must serve multi-tenants and particular T&C's are applicable to all.	The State will review all vendor-submitted terms and conditions and accept those that best meet the state's needs. We need to understand the architecture and separation of customers from a security perspective. Data must also remain in the Continental US.
4	Have you evaluated and/or been presented with demos/meetings from other e-signature vendors already year to date?	No

Question #	Vendor Question	The State's Response
5	Will you be open to a conversation/demo between key stakeholders and vendor - prior to the submission of a response to make sure that the vendor and state are on the same page as to need, functionality etc.?	Conversations/ demos will not be done prior to the bid submissions.
6	You mention that up to 65K transactions will be procured. Is that for the 1 st year or over a number of years? What do you see as the minimum amount of transactions purchased in the first year?	65,000 transactions are the current annual usage. We used historical figures in the RFP. We are unable to give the minimum amount of transactions the first year.
7	Will there be any need for on premise solution?	No, the State is seeking a SaaS solution We are not wanting to build an on-premise solution. This is a decentralized solution and need the Vendor to take care of operations, configurations and administration.
8	As the State intends to provide more than one Cloud Based Software solution, does the State currently offer solutions hosted in Azure? Are their contracts in place with Microsoft in this regard that can be leveraged?	The state is looking for a SaaS Solution offered by the vendor. The Vendor should use their own Cloud/Infrastructure and not the State's.
9	As the table only indicates up to 25 named user, can you confirm there are no more than 25 named users who will create forms templates and capture data on these forms for processing? Are the transactional numbers listed for public facing forms only or are these transaction numbers in lieu of named users?	At some point there will be a break even or business reason to move to transaction based pricing. Vendor must provide pricing up to 25 named users. Vendor can provide pricing for more than 25 if they want to. Vendor is encouraged to recommend when one solution makes more sense than the other. The vendor should identify costs for public facing form sign offs.
10	Is the list provided definitive? Are we to assume therefore that licenses for commodity databases such as SQL Server are not available via the state and thus must be licensed for this project separately?	We want a turnkey SaaS solution. Vendor's licensing should include all costs for providing that solution.
11	The cited Branding guide is protected by an ID / password challenge. Can the state please provide this to bidders?	Removed in #2 above.

Question #	Vendor Question	The State's Response
12	Can the state elaborate over what timespan the 95,000 transactions are expected? Is this annual expected usage? Does this include both internal named users as well as a Customer Facing Web Portal to Serve the public (non-employees) of the State?	This RFP initiative calls for an Indefinite Quantity Contract but typically, this is the estimated yearly amount. Yes, it will include both internal and external users.
13	Will the solution need to integrate with 3rd party signature software such as DocuSign?	No.
14	Will the solution need to integrate with a Content Management System such as Drupal or WordPress?	The solution will need to potentially integrate with content management systems. We have asked for connectors or the ability to integrate to Dynamics 365, Salesforce, SharePoint Online and on Prem. Solution provides Application Programming Interfaces (APIs) for integration with other Customer systems. Include any details on Application Programming Interfaces (APIs) provided.
15	How often would data need to be transferred to internally hosted systems? Hourly? Daily?	Hourly at a minimum, and if possible, in real-time.
16	Do you require form analytics and/or data visualization?	The State considers these "nice to have," but not required.
17	Will the solution need to have multilingual capabilities for forms in different languages?	Yes.
18	Any specific requirements for level of web content accessibility i.e. WCAG 2.0 A - AAA?	Yes, State requires the build be WCAG 2.0 AA compliant.
19	What is the preferred format for references?	Format of references is at the discretion of the vendor; however at a minimum, vendors are expected to include name, phone number/email, and title and company of the individual providing the reference.
20	Is there a specific Cloud Service Provider the State prefers for this RFP i.e. AWS, Azure, other...	The state is looking for a SaaS Solution offered by the vendor. The Vendor should use their own Cloud/Infrastructure and not the State's.
21	Does the State currently have usage analytics such as monthly traffic, average downloads, etc.?	The State currently uses Tableau and PowerBi. The State does require a rolled-up view of utilization both quarterly and yearly.
22	Have all of the existing forms already been converted to PDF format?	No.
23	Does each agency have an index or catalog of their forms?	No.
24	Does the current infrastructure facilitate network communication with all agencies using forms?	No.

Question #	Vendor Question	The State's Response
25	Do all forms reside on the same domain?	No.
26	Is there a predominant platform in use and if so what is it? (Windows, Unix, Ubuntu, etc.)	Windows Office 365.
27	Do all network subscribers currently have digital signatures	No.
28	Are all ad hoc work flows identified and documented throughout the enterprise?	No.
29	Does current Enterprise use Active Directory or some other directory service? If so, which one?	Most agencies use the State's Enterprise Active Directory Service (EADS) via SAML, but not all. However, all Agencies use NCID for Authentication.
30	Is there currently a predominant internet browser throughout the Enterprise or will vendor provide support for all browser types?	There is no predominant internet browser. Browsers should be N-1 and vendors should describe if the solution facilitates digital signing of documents via a computer web browser with modern browsers. Specify minimum software versions supported.
31	Is it an assumption that in the 12 months, all of the 95,000 transactions will have digital signature capability?	95,000 transactions is an annual estimate, but this will be an indefinite quantity contract. Number of transactions is not guaranteed.
32	Does NCID manage Enterprise Digital Signatures? If so, who is the point of contact?	No.
33	Does NCID manage all security groups?	NCID only does authentication, not application authorization.
34	Which directory service AD or is used?	The State's active directory (AD) service uses Microsoft Active Directory.
35	For pre-population, does the State have forms that already auto populate? If not, do all forms that need the pre-populate feature have business processes associated with them?	Some agencies may have forms that prepopulate, but this functionality is not available across the state.
36	Does the State know the location of the site where the current repositories for forms are stored? How many years has the current repository existed? What is the current size of it?	Each agency has a respective repository. Age and size are unknown.
37	Does the State know by location, region or area, the current number of reports being used in each area? If so, what is the approximate breakdown by location, region or area?	The State does not have this information.

Question #	Vendor Question	The State's Response
38	Will the State use their own existing service desk or will the vendor be required to establish service operations for Enterprise Forms Solutions?	The Vendor to provide support for the solution.
39	Will an online LMS style be a viable option for an Enterprise Solution?	Yes, Vendors are encouraged to provide multiple training options.
40	Will training be provided throughout the forms life cycle?	Yes, ideally training will include an array of users up to Administrator.
41	Is training the responsibility of the vendor or will the State facilitate their own training?	The State prefers the Vendor to assume training responsibility; the State is open to "train-the-trainer" or "on-demand training for all levels" types of environments.
42	What type of integration is the State looking for with NCID? Is this a method to authenticate citizens, or is this for internal users?	Users with an NCID should be able to authenticate. Non NCID users should be able to be involved in work flow and business process. The Vendor is encouraged to elaborate on what authentication methods can be provided for non NCID users.
43	Can the State elaborate on the intended use case for capturing a picture of the signature owner with the signature?	The ideal solution will capture a picture of the owner's signature and associate it with the actual signature.
44	Does the State have any restrictions around the graphical image of the signature? If so, what are they?	No.
45	Can the State elaborate on what is intended by capture speed and pressure? Is there a specific use case where this would be a requirement?	No.
46	Can the state provide additional information on the requirements for redlining?	Redlining will allow users in a workflow to make changes and have those changes be routed to the originator and all previous signers.
47	Do you require proven performance/experience in the state of North Carolina with state and local agencies? If not required, is it preferred?	No, per the RFP, preferred evaluation criteria consists of the Vendor's corporate background and similar experience, specifically the technical situations, specifications, needs, challenges, and opportunities.
48	Is there a small business preference?	No; however, pursuant to N.C.G.S. §§143B-1361(a), 143-48 and 143-128.4 and any applicable Executive Order, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, and disabled business enterprises.

Question #	Vendor Question	The State's Response
49	Is the state using the term "Digital Signature" and "Electronic Signature" interchangeably? All Digital signatures are electronic signatures, but not all electronic signatures are digital signatures.	Yes, we are used interchangeably.
50	Does the State prefer a vendor who has FedRAMP authorized Moderate who can handle PHI/PII for state agencies? Vendors that are FedRAMP authorized Low are not certified by FedRAMP to handle PHI/PII.	Data stored in the e-Forms/e-Signature Program may be classified from public up to Highly Restricted. Therefore, the e-Forms/e-Signature Program should be classified as NIST Moderate per the Statewide Information Security Manual and must be capable of receiving and securely managing data that is classified up to Restricted or Highly Restricted per the State's Data Classification and Handling Policy. To comply with policy, assessment reports such as the Federal Risk and Authorization Management Program (FedRAMP) certification, SOC 2 Type 2, and ISO 27001 are preferred and offered solutions already meeting these requirements are requested to include these reports as part of their submission.
51	Do you have required minimums for uptime?	No.
52	Regarding uptime statistics, would the State prefer for vendors to provide the following metrics?	Yes.
53	-Historical uptime for the last 3 months, 6 months, and 12 months	Yes.
54	-Uptime inclusive of maintenance windows	Yes.
55	-Average hours the system is scheduled to be down for maintenance	Yes.
56	Does the State prefer to have uptime reporting to be inclusive of maintenance windows?	Yes.
57	Does the State prefer a vendor to report	Yes.
58	If the state does mean, digital signatures, who will be the certificate authority? Is the state planning on being the certificate authority?	The solution can be electronic signature or digital signature. The state will not be the digital certificate authority. The solution shall produce an esigned pdf which is automatically trusted and validated by Adobe when opened by Adobe.

Question #	Vendor Question	The State's Response
59	Is the state looking for providers that provide the digital/e-signature, e-forms, and workflow capabilities under one brand?	Yes.
60	Can a vendor that supplies an e-form and workflow solution that integrates with solutions like Adobe Sign and DocuSign, submit a response for these sections of the RFP only.	We are looking for a turnkey solution like we have today which allows for forms and Signature.
61	Section III - Page 25 10d - Are NCDIT referring to the digital certificate that is wrapped around an electronically signed document?	The solution needs to generate an electronically or digitally signed PDF that is automatically verified as a valid e-signed PDF when opened by Adobe Reader.
62	Section III - 3.6 – The link to branding guidelines is password protected. Can you please provide us access to the branding guidelines referenced in the RFP document?	Removed in #2 above.
63	Does NCDIT require custom domains in their URLs?	All URLs must be https.
64	Section III - 3.11 – RFP States: <i>"Based on current usage, the State estimates that the solution will eventually accommodate over 95,000 transactions"</i> , Question: Over what timeframe?	Yearly.
65	Does the cost for back end integrations need to be included? If so, which integrations specifically need to have a price called out? If there are any integrations (non-implementation) for pre-built product integrations?	All costs should be specified for making the integration with NCID and various Connectors.
66	Do costs for annual support costs need to be called out in the response? If so, how detailed do we need to provide.	All Potential Costs should be supplied.
67	Do you need to know if there are any costs for onboarding or account management? Per hour or one-time charges?	All Potential Costs should be supplied.
68	If this is a state-wide implementation, will 96,000 transactions cover all interested agencies and is this an annual figure or aggregate for the term of the contract?	This number is an annual figure.

4. Failure to acknowledge receipt of this addendum may result in rejection of the response.

Check ONE of the following options:

- ☐ Bid has not been mailed. Any changes resulting from this addendum are included in our bid response.
- ☐ Bid has been mailed. No changes resulted from this addendum.
- ☐ Bid has been mailed. Changes resulting from this addendum are as follows:

Execute Addendum:

Vendor/ Offeror: Click here to enter text. RAIN GOVERNMENT LLC

Authorized Signature: Click here to enter text. Larissa Newman

Name and Titled (Typed): Click here to enter text. LARISSA D. NEWMAN, CAPTURE

Date: Click here to enter text. JULY 19th, 2018 MANAGER