Enterprise Collaboration Services

North Carolina Department of Information Technology

Enterprise Collaboration Services Service Level Agreement

Service Level Agreement

Version Control

Author/Change Agent	Version	Reason for Change	Date
Mark A. Moore / Suzanna Cary	1.0	Revised and updated SLA	06/19/2018
Suzanna Cary	1.1	Updated Team Name and O365 to M365	09/30/2020

Service Level Agreement

Contents

Service Level Agreement

Objective

This Service Level Agreement (SLA) establishes the framework for addressing the administration, management, support, and use of Microsoft 365 (M365) & Exchange Online; including current and future features implemented to the M365 Enterprise. All sections of the Agreement are subject to audit by the M365 Subject Matter Expert (SME) or designee. This Agreement is considered a living document and shall be updated and revised as required or as needed where changes in features, updates, processes, and security concerns dictate.

The term "Best Practice" defines methods that are strongly recommended to avoid increased support issues due to design, limitations, or overall functionality.

The M365 SLA describes the IT Service, documents the Service Level Targets, and specifies the responsibilities of both the Department of Information Technology (DIT) and the Customer. These include:

- The core Service Description
- (Optional) Definition(s) of Customer-specific Service Levels, such as enhanced levels of support
- (Optional) Specific Customer Requirements; including any mutually agreed and/or binding Customer-specific requirements and terms. These may be referenced within the core verbiage of this SLA, or referenced to an accompanying, signed Memorandum of Understanding (MOU).

This SLA is entered into by and between DIT Enterprise Collaboration Services (UC) and the {Customer/Agency Name}, effective upon the date of signature by DIT to document the understandings, obligations, and agreements of the Parties regarding {Customer/Agency} Email, Email Archiving, Calendaring, eDiscovery and any additional features.

Disclaimer

Regarding content and/or scope deviations between this document and the established DIT Global Service Levels policy, this Service Level Agreement takes precedence, once properly executed. If there are any additional or accompanying MOU or other contractual vehicle properly executed yet having contradictory content or scope specific to this Service or requirements, this said contractual document takes precedence.

M365 & Exchange Online Framework

DIT operates one Production M365 tenancy in the Government Cloud and one Test tenant. The following applications are currently in the Microsoft 365 environment:

- Exchange Online
- Teams

- One Drive for Business
- Office Pro Plus
- SharePoint Online
- Project Online
- Power Bi
- Intune MAM
- Dynamics 365
- Power Apps
- Power Automate
- Azure

Summary of M365

M365 is a Subscription Service provided by Microsoft through DIT. If warranted, by means described within the SLA, DIT can request financial compensation from Microsoft for breach of SLA. If accepted Microsoft will send refunds directly back to the Agencies who have purchased the licenses. Agencies can choose from a full suite of products and services that meet their business requirements and costs. The state has moved to Secure Productive Enterprise (SPE) E3 suite for users. This Stock-Keeping Unit (SKU) is now called the "Microsoft 365" E3 Enterprise Mobility Suite. For email only accounts, an Exchange Online Plan 2 is needed to get Email and Archiving. Additionally, some Agencies have purchased E1 Web Only Apps with Exchange Online Plan 2 (EOP2) or Exchange Online Archive. Email Archive is included in E3 and EOLP2.

Service Description

Visit the Microsoft website to review the M365 Service Descriptions.

- "Microsoft 365" Full Suite (E3) — Office, Email/Archive, SharePoint, OneDrive, Skype for Business
- Web Access Only (G1) — Office Web apps, Outlook on the Web, SharePoint, OneDrive, Skype for Business, Archive in Web Access only
- Email Only — via Outlook on the Web, Exchange Online Plans (EOLP), Archive in Web Access only.

Note 1: M365 Exchange is an online service. DIT and the Agencies are subscribers via the licenses purchased to access the service. There are multiple access methods for this service, such as Outlook, Outlook Web Access (OWA), and Mobile. Consequently, DIT Service Desk tickets for service issues with unmanaged devices will be treated as a Best Effort service with no specified SLA. If the device is managed by DIT, the ticket will be assigned to the Consumer Platform Support Group within their SLA Agreement. If the Exchange Online Service has an issue that can be verified on the M365 Service Health

Dashboard, then the ticket will be treated as an Incident. For most issues with Outlook, OWA is usually still available as a workaround. *See* Support Matrix.

Note 2: Email is not a guaranteed delivery service. When an email is sent, there is no guarantee it will get to the destination due to systems beyond DIT control. Typically, the user will get a Non-Deliverable Report (NDR) warning, but not always.

Note 3: Exchange Online Limits

Exchange Email Service

The Microsoft Exchange Email Service provides an enterprise-wide email and calendaring solution that is highly available and reliable, feature rich, and cost effective to use for State agencies and local government entities. The Service runs on the Microsoft Exchange Server 2016 platform and provides customers with efficient access to email, calendar, attachments, contacts, and more. Service support is provided by experienced and professional personnel focused on "Best-in-Class" customer service and satisfaction.

Email, Calendars, and Protection

Agencies have Government-class Email through Exchange Online Services. This service provides Email, Archive, and Protection with the rich and familiar Outlook experience users are accustomed to. Users can access these services from their desktop web browser using Outlook for the Web (OWA) and mobile devices. Each user gets a 100 GB mailbox and can send attachments up to 25 MB. Email Archive is unlimited and all mailboxes are put on legal hold for compliance. Retention policies can also be applied. Shared calendars let users see when others are free or busy.

- Exchange Online Service Description
- Exchange Online Limits

The Exchange Email Service includes:

- Integrated Email and Calendar function
- 100 GB of Email storage per user, with unlimited archive
- Microsoft Exchange Online
- Integration with the NC Identity Management system (NCID)
- Redundant and load balanced configuration
- Disaster Recovery/Business Continuity infrastructure
- Antivirus and Anti-Spam solutions
- Internet browser access for Email: Outlook Web Access (OWA)
- Centralized and personal address books
- Folder creation and management for messages
- Native file format attachments; i.e., Word, Excel, etc.

- Outlook 2013 and Outlook 2016 access from anywhere via RPC/HTTPS-Outlook Anywhere (SSL encapsulated client connections). Agencies should use the current Office Click to Run software to utilize all production functionality.
- Centralized administrative website for commonly performed functions
- Meeting scheduling for individuals, groups, and other required resources such as conference rooms and conference numbers
- Personalized or shared daily notes/tasks
- Share/view calendar entries with others
- Designate rights for others; i.e., administrative assistants, to create meetings on your behalf
- Mobile device wireless synchronization via Outlook Mobile App (*see* Intune Service)
- Email Archiving (*see* Email Archiving Service for more details)
- Requirements include:
    - For Outlook users—an NCID account, Outlook 2013 or higher, and Windows. Office/Outlook 2016 or later is recommended.
    - For OWA users—Bowsers that are N-1 or higher are recommended, but OWA will function in a limited fashion with older browsers

eDiscovery

eDiscovery in M365 is accessed through the Security and Compliance Center admin portal. eDiscovery administrators are chosen by the Agency secretary, subject to approval by the SCIO. It is the Agency's responsibility to maintain a list of administrators, especially in times of political transition. After eDiscovery administrators are chosen they must complete training. To request training, send an email to dit.incidents@nc.gov.

Email Archiving Service

The Email Archiving Service provides archiving of all Exchange mailbox content, including messages, calendar items, contacts, Skype for business conversations, and tasks for the 5-year period specified by Executive Order 12. This Service is based on eDiscovery software. Coupled with a robust physical storage solution, eDiscovery provides significant deduplication capabilities, resulting in efficient use of disk space.

eDiscovery archives all items in real time as they arrive in or are sent from a user's mailbox, and archives changes in state, such as a message manually moved from one folder to another within the mailbox. Exchange users have access to their own archived data through the Archive folder which appears in their Outlook client or OWA browser session. In this folder, users can search their archived data in seconds, and view message history and deleted items.

Users specifically designated by agency leadership can perform eDiscovery for legal purposes and public records requests using an additional eDiscovery client.

The Email Archiving Service includes:

- Archiving and 5-year retention of all mailbox content
- Access to a user's own archived data through the Archive folder in Outlook and OWA

Intune Mobility Application Manager Service

The Intune MAM Service enables customers to connect wirelessly to their Microsoft Exchange email and calendar account via smartphone or tablet devices. This highly available and feature rich service provides customers with efficient mobile access to email, calendar, attachments, contacts, and more. Service support is provided by experienced and professional personnel focused on "Best-in-Class" customer service and satisfaction.

Exchange Online Protection and Encryption

Exchange Online Protection defends against spam and malware. It provides advanced security by eliminating threats from known viruses and 99% of spam before they reach the firewall. Exchange Online includes:

- Anti-Spam and Anti-Malware Protection
- Exchange Online Protection
- Exchange Online Protection overview

Exchange Online Encryption:

- Encryption in Microsoft 365
- Service Information for Microsoft 365 Message Encryption
- Microsoft 365 Message Encryption FAQ

Email Encryption Service

The Email Encryption Service Includes:

- Ability to send secure email to anyone on any email system (encryption "in transit")
- Secure Receive and Reply for message recipients
- Zero desktop footprint (no software or add-in installation is needed)
- Built-in content scanning capability (can encrypt based on specific message content)

See Encryption in Microsoft 365

Relay and SPAM Filtering Service

The filtering process occurs through a SPAM Filtering Service and then M365. DIT's SPAM Filtering Service incorporates a multilayered approach to filtering email for spam and viruses. This helps protect employees by scanning email and eliminating threats such as viruses, worms, malicious content and attachments, and other junk mail before they reach the end user.

DIT offers the same antivirus/anti-spam protection to local governments and other State agencies that is provided to our Exchange customers.

Locals still have admin access, while state agencies have read-only access. Whitelist/Blacklist requests must be made via service request through the Service Desk.

For hosted email Agencies, this service is included in the monthly support rate. For non-DIT hosted email there is a charge for this service.

The Relay and Filtering Service includes:

- Comprehensive virus scanning and spam filtering for all Email messages
- Email message relay capabilities for any Email system via Simple Mail Transport Protocol (SMTP)

Data Loss Protection

Data Loss Prevention (DLP) is important for enterprise message systems because of the extensive use of Email for business-critical communication, which can include sensitive data. With M365, customers own and control their data. The data is not mined or used for advertising.

For more, *see* Email Encryption and DLP.

Email Management / Admin Portal

The Email Admin Portal provides the day to day management for DIT, Agencies, and the Service Desk. Below is a list of what each role can perform. Each Agency should have one or more Email admins identified to perform on-/offboarding activities like the NCID role, but not necessarily the same person as the NCID admin. The NCID and Email admins must work together to add, modify, and delete users in the State Email system.

Agencies must submit a Service Request to add and delete email admin access. Once access and training have been accomplished they can login to the Email Admin Portal.

Agency Administrator Functions

1. **Calendar Resource**
   a. Add
   b. Delete
   c. Manage
      i. Display name
      ii. Primary SMTP Address
      iii. Admin Group
      iv. Automatic processing
      v. Allow recurring meetings
      vi. Booking window (365 days)
      vii. Schedule Only during work hours
      viii. Delegates
      ix. Forward requests to delegates
      x. Users with “Book in” privileges
      xi. Book in policy
      xii. Manage Calendar Permissions
      xiii. Calendar automatic processing
      xiv. Calendar allow recurring meetings
      xv. Calendar booking window (180 days)
      xvi. Calendar Schedule only during work hours
      xvii. Calendar Delegates
      xviii. Calendar forward requests to delegates
      xix. Calendar book in policy

2. **User**
   a. Add MBX
   b. Delete MBX
   c. Manage MBX
      i. Display Name
      ii. Name Alias
      iii. Primary SMTP Address
      iv. Secondary SMTP addresses
      v. Mail aliases
      vi. Bill Code
      vii. Disable account
      viii. Send-On-Behalf-Of Permission
      ix. Mailbox ‘Full Access’ right
      x. “Send-As” permission
      xi. List group membership

3. **Add Service accounts** - Agencies cannot add Service Accounts but they can manage them once created. To submit a Service Request, send an email to dit.incidents@nc.gov
4. **Manage Service Account**
    i. Display Name
    ii. Primary SMTP address
    iii. Secondary SMTP address
    iv. Admin group
    v. Bill Code
    vi. Disable account
    vii. Change password
    viii. Send-On-Behalf-Of delegates
    ix. Mailbox "Full access" right
    x. "Send-As" permission
    xi. See MBX Storage
5. **Mail contacts**
    a. Add
    b. Delete
    c. Manage
        i. Display Name
        ii. External Forward Address
        iii. Primary SMTP address
6. **Distribution Group**
    a. Add
    b. Delete
    c. Manage
        i. Display name
        ii. Primary SMTP Address
        iii. Secondary SMTP addresses
        iv. Grant send-on-behalf-of privileges to
        v. Accept messages only from internal users
        vi. Accept messages only from these users
        vii. Reject messages only from these users
        viii. Accept messages only from these distribution groups
        ix. Reject messages only from these distribution groups
        x. Send delivery report to the sender of the message
        xi. List/add/remove members
    d. Display dynamic distribution group
7. **Mail Security Group**
    a. Add
    b. Delete
    c. Manage

i. Add/remove members

Super Administrator Functions

8. **M365 License reports** (New Function and admins can generate)
   a. M365 Licenses assigned by
      i. Agency
      ii. One or more divisions/admin groups in an agency
9. By default, all new user accounts are set up as a G3 license. If a service account is requested, it will get a EOLP2.

Mailman Email Distribution List Management Service

The Email Distribution List Management Service uses Mailman software running on Red Hat Enterprise Linux 4. Mailman is integrated with the web, making it easy for users to manage their accounts and for list owners to administer their lists. Mailman supports built-in archiving, automatic bounce processing, content filtering, digest delivery, spam filters, and more.

More Information:

- Mailman Administrator login
- Mailman Documents

The Distribution List Management Service provides customers with a low-cost and highly secure method of maintaining Email distribution lists. Key to the Service is the ability to moderate (approve) postings to distribution lists. Auto-subscribe/unsubscribe features are also provided. The Service offers an open standard solution to state and government agencies that is highly available and reliable. Service support is provided by experienced and professional personnel focused on “Best-in-Class” customer service and satisfaction.

The Mailman Email Distribution List Management Service includes:

- Mailman software used for Email Distribution List Management
- Users can subscribe or unsubscribe to a list
- List members can be inside or outside of the DIT Email system
- Any list can be moderated by a moderator or list administrator
- Posting a message to a distribution list can be restricted to only the list members
- Options for individual Email message delivery posted to the list, or a “digest” message that combines multiple postings
- Archive option permits posted messages to be saved via a web browser interface
- Easy to use and administer by non-technical personnel

Service Commitments

Standard Support Hours

Enterprise Collaboration Services are available to customers 24/7/365, excluding planned outages, maintenance windows, and unavoidable events. Maintenance windows are used only when needed for scheduled changes that have been implemented through the DIT Change Management Process. In addition to the standard DIT maintenance windows, site-specific and service-specific changes may be coordinated with customers at non-standard times.

- For Critical and High Priority Agency or Enterprise-wide Incidents, support is available 24/7
- For Low or Medium Priority End User Incidents, the Service Desk M365 SMEs are available 24/7 for First Level Support. Second and Third Level Support for Enterprise Collaboration Services is available from 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding State Holidays.
- Request response times are within 5 business days.

Incident Prioritization Model with Response Times

Priority	Target Acknowledgement Response (OLA)	Target Status Update (OLA)	Target Customer Status Update (SLA)	Target Resolution (SLA)	Target % of Calls Resolved on Time
Critical	15 minutes	Every 30 minutes by assigned working team until resolved	Every 60 minutes or as agreed upon with the customer(s)	4 hours or less	90%
High	30 minutes	Within 1 hour, then every hour thereafter by assigned working team until resolved	Every 2 hours or as agreed upon with the customer(s)	8 hours or less	90%
Medium	2 hours	Within 3 hours	Every 6 hours or as agreed upon with the customer(s)	24 hours or less	90%
Low	1 business Day	1 business day	Daily	3 business days	90%

Maintenance Windows

Enterprise Collaboration Services follow the DIT Standard Change Management maintenance windows:

- 4:00 a.m. to 12:00 p.m. on Sundays
- 4:00 a.m. to 7:00 a.m. on Thursdays

Roles and Responsibilities

Overall Architecture

The state maintains on-premises Active Directory and Exchange Servers (ADFS) for identity of all users, federated to ADFS and synced to the Cloud via Forefront Identity Manager (FIM) to sync with Azure Identity. The state currently has an in-house developed Distributed Admin tool for mail (NC Mail Admin Portal) to manage the M365 environment in terms of mail provisioning, license management, and billing. Agencies are given access to admin groups via an exchange attribute to manage their environment and users. State government is organized into agencies and each agency has one or more divisions/admin groups. Divisions/admin groups are set up as Operating Units (OU) and nested OUs in Active Directory (AD). There are roughly 400 administrators across the State who manage mail provisioning, and 10 Super admins on the email staff that can manage all domains. There is also a Service Desk group that has more capabilities than the Agency admins but not as much privilege as the Super admins.

- One Tenant 40+ domains with multiple Admin groups per domain
- Centralized ADFS/FIM Solution
- Licenses are pooled, assigned, and reported by Agency and admin group
- Email Admin Tools allow for multiple roles (Global, Service Desk, Agency Admin)
- Agencies must manage their purchased and consumed licenses. Failure to manage licenses will cause a shortage of licenses.

DIT Responsibilities

- Provide Escalated Support after Agency does triage with their admins or Service Desk
- Provide day to day monitoring and management of the M365 Platform and DIT services
- Assign Agency Users to Licenses. The M365 Service does not provide the licensees. Licenses are provided by the Agency. For Managed Desktop customers, DIT provides the M365 License. Use of Visio and Project is purchased by the Agency.
- Provide links to Online Training Resources and Roadmap information
- Provide a tool to manage on-/offboarding of users
- Provide a user-friendly license report for Agency consumption located here.

- Maintain contracts for filtering support/service and Microsoft Premiere Services
- Provide a SharePoint site for M365 services, Community of Practices, Service Offered, and Announcements

Agency Responsibilities

- Maintain Email per agency's retention schedules and policies
- Review all DIT M365 Service information in this document and in SharePoint (This will be the main source of support for Agencies)
- Manage their Purchased vs. Consumed license
- Provide and maintain a primary and back-up Email admin
- Email admin will provide 1st level support and all on-/offboarding activities
- Secretary of the Agency must identify and maintain an eDiscovery admin
- Periodically review the M365 Support and Announcement Page
- Ensure all agency licensing is in place and available, including Windows server CALs
- Agree to and understand the Support Matrix of the service
- Provide Application testing for integration/dependencies with M365. Application owners should gauge their agencies' application remediation required for moving to M365.
- Deploy and maintain updates on OS, browser, and Office. The Office version used should be Click to Run M365 and be on the Monthly Channel for updates. Windows 10 and Office 2016 are highly recommended.
- Test Office deployment options and customize options for the Agency
- Provide user training and communications to employees for the M365 Service
- Maintain security best practices
- Work with Security liaison on email monitoring requests, whitelist, blacklist, and filtering requests
- Communicate to their users about the Email service, specifically best practices like Encryption and DLP.
- The primary contact for the end user should be the Agency's help desk, which can contact DIT if escalation is required.

Service Level Agreement Scope

This agreement specifies only the standard operational service commitments and responsibilities of DIT and DIT Customers. Customer-specific deviations from these commitments and responsibilities will be specified in an accompanying Memorandum of Understanding (MOU). Service rates are outside the scope of this agreement and are specified in financial documents.

Signatures of Approval and Agreement Date

WHEREFORE, intending to be bound hereby, this Service Level Agreement is executed by the undersigned authorized representatives of each Party, effective as of the date of execution of all Parties hereto.

Agency Head or Designee:

Name	Title	Signature	Date

Agency Chief Financial Officer:

Name	Title	Signature	Date

State Chief Information Officer:

Name	Title	Signature	Date
Name	Title	Signature	Date