NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

State of North Carolina

Statewide Data Classification and Handling Policy

Version 2.0

February 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
June, 2025	1.0	Revised	Annual Review	Martha K. Wewer
February, 2026	2.0	Revised	Update of data classification categories	Martha K. Wewer

Document Details

Department Name	Office of Privacy and Data Protection
Owner	Martha K. Wewer
Title	Statewide Data Classification and Handling Policy
Publication Date	February 2026
Next Release	Reviewed Annually
Document Type	Policy
Version	2.0

Table of Contents

Introduction

Purpose

This policy establishes a statewide data classification framework to ensure consistent identification, protection, and handling of State data. It classifies data based on the potential impact of unauthorized access, loss, theft, or corruption and provides guidance on appropriate security measures. By implementing this framework, State agencies, departments, and other entities, can safeguard personal information, comply with legal and regulatory requirements, and mitigate risks associated with data exposure.[1]

Owner

Statewide Chief Privacy Officer, Office of Privacy and Data Protection (OPDP)

Scope

This policy applies to all North Carolina state agencies, departments, local governments, institutions, and other entities that are not specifically exempt under Article 14 of N.C. General Statute Chapter 143B. It governs the classification, handling, and protection of data processed, stored, or transmitted by these entities. Additionally, any third-party vendors, contractors, or service providers handling State data must comply with this policy's requirements.

Pursuant to N.C.G.S. 143B-1320(b), any exempt entity that has properly elected to participate in information technology programs, services, or contracts offered by NCDIT, including information technology procurement, must do so in accordance with the applicable statutes, policies, and rules governing those offerings, including this Statewide Data Classification & Handling Policy.

Definitions

Unless specifically defined in this policy, terms are defined in the Statewide Glossary of Information Technology Terms.

[1] See NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, for a discussion of a risk-based approach for protecting data.

Part 1. Data Classification

Policy

All State data must be classified and maintained in a manner that ensures confidentiality, integrity, and availability while making it accessible only to authorized users. Data classification shall be based on the level of sensitivity, legal and regulatory requirements, and potential risks associated with unauthorized disclosure, modification, or loss. This policy will be reviewed on an annual basis.

Annual Review

All data classifications must be reviewed, at a minimum, every year or when there is a significant change that may impact the security posture of the data and/or system requiring a re-evaluation. A significant change includes but is not limited to data aggregation/commingling or decoupling of data. A re-evaluation may also occur when a system classified as low or medium risk is later interconnected with a system classified as high risk.

Data Classes

All State data must be classified based on its level of sensitivity and potential impact in the event of unauthorized disclosure, modification, or loss. Data classification shall follow this four-tier system.

1. **Public (formerly Low Risk)**
2. **Internal (formerly Medium Risk)**
3. **Confidential (formerly Medium Risk)**
4. **Restricted (formerly High Risk)**

The classes determine the level of security that must be placed around the data. The data creator or steward, defined in Part 2 Data Classification Roles and Responsibilities, is responsible for classifying information correctly.

If data or systems include multiple classifications, the classification must default to the highest level. For example, a system that stores, processes, transfers or communicates Public and Internal data is classified as Internal and subject to the higher access controls and data handling restrictions.

Data Classification System

Public (Formerly Low Risk)

This is the lowest level of sensitivity within the classification structure. Information labeled as **Public** is available and intended for public access. This type of information and data, if exposed to unauthorized parties, would have no impact on the agency's reputation, compliance requirements, or ability to achieve strategic goals. This information does not require protection mechanisms. However, care should always be taken to use all State data appropriately. Examples of Public data are information that is appropriate for general access by the public, public press releases, marketing materials after release, or public job postings. Public data includes publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and information made lawfully available to the general public from federal, state, or local government records. (See N.C.G.S. 75-61(10)).

Internal (Formerly Medium Risk)

Internal data is the second highest level of sensitivity. This is information typically used within the agency and not for public sharing. Most documents are classified as Internal within the organization, and most

employees would have access. This type of data, if exposed to unauthorized parties, would have a very limited impact on an agency's reputation, compliance requirements or ability to achieve strategic goals. Internally classified data does not contain direct identifiers. Often, the effects of the loss of data can be recognized in very subtle ways and may not lead to clear negative consequences causing confusion due to lack of context or minor reputational harm. The following types of data must be classified as Internal. This is not a complete list and is subject to legislative changes.

1. Agency policies, standards, guidelines, and procedures not yet published (except those related to physical or technical security)
2. Drafts of yet-to-be published documents
3. Employee work schedules and duty assignments
4. Internal newsletters
5. Training materials

Except for specific work assignments, most Internal data would be subject to a public records request pursuant to N.C.G.S. Chapter 132 (after consultation with appropriate legal counsel).

Confidential (Formerly Medium Risk)

Confidential data is the third highest level of sensitivity. This information is limited to a small audience on a "need-to-know" basis. Agencies should determine what constitutes "need-to-know," but this type of data, if exposed to unauthorized parties, would have high impact and could cause regulatory or legal fines, inability to recruit talent, loss of an employee or constituent or agency confidence, damage in vendor relationships or breach of contract. Those factors should be considered when determining classification but at a minimum, information that is confidential is restricted to only those individuals who need access to the information to do their job. Data classified as Confidential may contain direct identifiers. Confidential data refers to all information about the organization, its operations, clients, or employees that is subject to reasonable efforts by the organization to maintain its confidentiality and that is not typically disclosed by law to people who are not affiliated with the organization.

1. **State Employee Personnel Records** – Information that is confidential pursuant to N.C.G.S. 126-22. Any unauthorized discussion, disclosure, and/or dissemination of confidential applicant/employee information is a misdemeanor under N.C.G.S. 126-27.

2. **Trade Secrets** – Trade secrets are defined in N.C.G.S. 66-152(3), and generally comprise information that is owned by a person, has independent value derived from its secrecy and which the owner takes measures to protect from disclosure. Misuse or misappropriation of a trade secret provides the owner a right of civil action (N.C.G.S. 66-153). The declaration of "trade secret" or "confidential" must be made at the time of the information's initial disclosure to a public agency (N.C.G.S. 132-1.2(1)(d)).

3. **Student Records** – The Federal Educational Rights and Privacy Act (FERPA) prohibits the disclosure of personally identifiable information derived from education records without a permissible exception defined by the law. The prohibition applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Schools may disclose, without consent, directory information (name, address, telephone number, date and place of birth, honors and awards and dates of attendance), however, the schools must inform parents and eligible students of such disclosure and allow for opting out of such disclosure. In addition, under N.C.G.S. 132-1.1(f), records maintained by the Community Colleges System Office or any community college, which contain personally identifiable information from or about an applicant for admission to one or more constitute institutions or to one or more community colleges called "Personally Identifiable Admissions Information" shall be confidential and not subject to public disclosure.

4. **Security Features** – Information that describes security features of electronic data processing systems, information technology systems, telecommunications networks, or electronic security systems – including hardware or software security, passwords, or security standards, procedures,

processes, configurations, software, and codes – is confidential (N.C.G.S 132-6.1(c)). This includes policies, procedures, standards, and guidelines related to the physical and technical security of the state.

5. **Sensitive Public Security Information** – As defined in N.C.G.S. 132-1.7, sensitive public security information includes information containing specific details of public security plans and arrangements or the detailed plans and drawings of public buildings and infrastructure facilities. Sensitive public security information also includes plans to prevent or respond to terrorist activity, to the extent such records set forth vulnerability and risk assessments, potential targets, specific tactics, or specific security or emergency procedures, the disclosure of which would jeopardize the safety of governmental personnel or the general public or the security of any governmental facility, building, structure, or information storage system.

   By law, information relating to the general adoption of public security plans and arrangements, and budgetary information concerning the authorization or expenditure of public funds to implement public security plans and arrangements, or for the construction, renovation, or repair of public buildings and infrastructure facilities are not sensitive public security information and should be classified as Public.

6. **Financial and Strategic Planning Records:** Information related to agency financial projections, budgets, legal proceedings and investigations not covered by attorney-client privilege or work product and forecasting assumptions is confidential.

Restricted (Formerly High Risk)

Restricted data represents the highest level of sensitivity and presents the highest risk to the State, agencies, and its constituents if disclosed or compromised. Access to this information is restricted to a limited audience. Restricted data is likely regulated by State or Federal law. This type of information, if exposed to unauthorized parties, would have the most significant impact on the reputation of either the State or constituent directly, may have significant compliance implications (fines, damages, legal action), detrimentally effect the State's ability to achieve strategic goals, impact market value, risks significant decrease in profitability, loss of market share, or present a threat to the health and safety of the State, it's systems, and/or constituents.

Restricted data includes the following: State agencies that receive, transmit or store State data that is identifiable need to ensure proper safeguards are in place to reduce the probability of unauthorized access and disclosure. Identifiable information or indirect identifiers coupled with other identifying information requires stricter handling requirements because of the increased risk to an individual if the data is compromised. This would include political opinions, racial or ethnic origin, religious or philosophical beliefs, and trade union membership.

Note: Please refer to the Statewide Glossary of Information Technology Terms for a concise definition of Personal Identifiable Information (PII) or see N.C.G.S. 75-61(10).

1. **State and Federal Tax Information (FTI)** – FTI is any return or return information received from the Internal Revenue Service (IRS) or secondary source, such as from the Social Security Administration (SSA), Federal Office of Child Support Enforcement, or the Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information. State and local tax information is defined in N.C.G.S. 132-1.1(b) and N.C.G.S 105-259(a)(2).

2. **Payment Card Industry (PCI) Data Security Standard (DSS)** – PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personal identification numbers, passwords, and card expiration dates.

3. **Protected Health Information (PHI)** – PHI is confidential health care information for natural persons related to past, present, or future conditions, including mental health information. This information is

protected under the same controls as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and state laws that address the storage of confidential state and federal personally identifiable health information that is protected from disclosure.

4. **Criminal Justice Information (CJI)** – CJI applies to confidential information from Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS). CJI is data necessary for law enforcement and civil agencies to perform their missions, including but not limited to biometric, identity history, biographic, property, and case and incident history data.

5. **Social Security Administration (SSA) Provided Information** – Information that is obtained from the SSA. This can include a Social Security number verification indicator or other PII data.

6. **Driver's Privacy Protection Act (DPPA)** - **DPPA definition applies exclusively to data maintained by the North Carolina Division of Motor Vehicles and dictates permissible disclosures and uses under federal law**. The DPPA governs how the NCDMV may disclose personal information from driver records. This law defines "personal information" and "highly restricted personal information" in a manner distinct from North Carolina's Statewide Data Classification and Handling Policy. Data classified under DPPA is subject to 14 specific permissible uses (e.g., law enforcement, insurance underwriting, vehicle recalls). DPPA does not override or change these classifications. It only regulates disclosures and uses specific to NCDMV data. Therefore, the State Data Classification and Handling Policy should remain the governing framework for how all state agencies classify, store, and protect data. Further information concerning this body of law can be found here. (*See* 18 U.S. Code § 2721).

7. **Controlled Unclassified Information (CUI) -** Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable Federal law, regulations, and government-wide policies. State agencies may handle CUI when they are acting as a contractor with a Federal agency. It is the responsibility of the Federal agency to communicate with the State agency regarding the type of CUI, any required labeling and third-party handling. CUI shall be treated as "Restricted" and therefore all access control, transmission, storage and disposal requirements apply to CUI unless otherwise indicated by the Federal agency.

Summary Table

The following table summarizes the four data classes.

	Data Classification			
	Public	**Internal**	**Confidential**	**Restricted**
Description	Available and intended for public access.	Typically used within the agency and not for public sharing. Most documents are classified as Internal within the organization, and most employees would have access.	Often limited to a small audience on a need-to-know basis.	Represents the highest level of sensitivity and presents the highest risk if disclosed. Access to this information is restricted to a limited audience.
Types	• Information on publicly accessible websites • Routine correspondence • Employee compensation • Press releases (final) • Job postings	• Employee work schedules and assignments • Administrative records • Internal newsletters • Drafts of documents not yet published (press releases, draft communication, draft policies)	• Business unit plans • Security features • Sensitive public security information • Draft versions of agency's annual/quarterly reports • Forecasting assumptions	• Personally identifiable information • PCI data security standards • PHI/HIPAA • Criminal justice information • State and federal tax information

	Data Classification			
	• Published policies, standards, procedures (excludes those related to physical or technical security) • Work email addresses	• Training materials not created for public use • Personal email addresses • Home addresses	• Personnel Records (not compensation) • Ongoing or disposed legal proceedings and investigations • Budget information • Source code and detailed architecture • Policies and guidelines related to physical or technical security	• Conflict of Interest disclosure • Disclosed financial data • Social Security Administration-provided information • Attorney-client communications • State employee human resources records • Driver's information located within NCDMV • Controlled Unclassified Information (CUI)

Table 1. Data Classification Summary

Part 2. Data Classification Roles and Responsibilities

The following roles and responsibilities are established for carrying out this policy:

- **Data Owner (Data Controller) –** The agency CIO is the Data Owner for their agency's data except data owned by Federal agencies, the N.C. General Assembly, the Department of Justice and the University of North Carolina System and its constituent institutions.

  Data Owners are responsible for the classification, protection, use and quality of one or more datasets within an organization. This responsibility includes, but is not limited to, ensuring that:

  - A system is in place for classifying data, assessing risks, and adequately defining the level of protection for the information which the State collects;
  - Proper security measures have been created to support the safeguarding of the State data;
  - Overseeing the administration of data usage to ensure compliance with state and federal privacy laws.

6. **Data Steward –** The Office of Privacy and Data Protection serve as the Data Stewards at the enterprise level, while the state agency's Privacy Liaison are Data Stewards at the agency level. Data stewards are staff members assigned by the Data Owner with assigned or designated operational-level responsibility for information management. Data stewards are responsible for policy implementation issues, for ensuring data is properly classified, and appropriate security measures are followed in accordance with the data's classification. While Data Stewards do not own the data, they have a thorough understanding of how the data needs to be documented, stored, and protected and can provide rules for the use of data or data derivatives. Data Stewards also ensure that all vendors and agencies follow state and federal privacy laws.

7. **Data Custodian[2] –** Data Custodians are personnel (e.g., IT and operations) who deal with the movement, security, storage, and use of data. They are responsible for providing a secure infrastructure in support of the data, including but not limited to providing physical security, backup and recovery processes, granting access privileges to system users as authorized by

[2] As used in this policy, the meaning of Data Custodian is different from N.C.G.S. 132-2 and N.C.G.S. 132-6. Those statutes define the legal custodian of records as the "public official in charge of an office having public records" and the "agency that holds the public records of other agencies solely for purposes of storage or safekeeping or solely to provide data processing."

data stewards or their designees, responding to security threats or breaches, and implementing and administering security controls over the information.

8. **Data User –** Data users are individuals (e.g., employees, contractors with access) who need and use data as part of their assigned duties or in fulfillment of assigned roles or functions. They extract value from the data to draw insights for business decision-making. Data users generally interact with other members of the data governance team, such as the Data Custodians and Data Stewards, to understand and use data. Individuals who are given access to public, internal, confidential and restricted data have a position of special trust and as such, are responsible for following the appropriate security measures implemented to protect the security and integrity of the data.

9. **Data Processors –** Data Processors are any third party (e.g., vendor/contractor, cloud service provider, IT contractor, consultant) that processes data on behalf of the state agency.

   They must follow all security, compliance, and contractual requirements outlined by the State. They cannot use or share data beyond the contractually agreed-upon purpose. Furthermore, they are required to report all security incidents and breaches in accordance with contractual requirements, state laws, or applicable federal regulations.

10. **Data Subjects –** Data Subjects are any persons (e.g., individuals whose data is collected) whose personal data is collected, processed, or stored by the state. This may include residents, employees, contractors, vendors, or customers of state services. Data Subjects may have rights under applicable privacy laws, such as access, correction, deletion, notice or restriction of their data. Data Owners or Data Controllers are responsible for establishing a process to comply with data subjects' rights requests where applicable.

Part 3. Safeguarding Data

Labeling

All data must be labeled to reflect its classification. Recipients of information must maintain an assigned label and protect the information.

If a storage volume or information source contains multiple classifications, then the highest classification shall appear on the label. Data labeling may be automated where possible or done manually but remains the responsibility of the Data Owner. Derived data inherits the highest sensitivity of the inputs unless a documented de-identification standard is met.

Unless noted, the controls and labeling requirements for production and lower environments are the same.

If known, the applicable statute shall be cited on the label. For example, "Confidential per N.C.G.S. 132-6.1(c)".

The following table summarizes labeling requirements for different classes of data.

Media	Classification			
	Public	Internal	Confidential	Restricted
Electronic Media Email/Text Recorded Media CD/DVD/USB (Soft Copy)	Sender should select "Public" in Outlook.	Sender should select "Internal" in Outlook for emails. Body of the email should contain "For Internal Use Only." External **and** Internal labels on media	Sender should select "Confidential" in Outlook for emails. Creation Date Applicable Statute, if known i.e. "CONFIDENTAL per N.C.G.S. §132.6.1(c)" External **and** Internal labels on media Email – Beginning of Subject Line	Sender should select "Restricted" in Outlook for emails. Creation Date Applicable Statute, if known i.e. "RESTRICTED per N.C.G.S. §132.6.1(c) External **and** Internal labels Email – Beginning of Subject Line (See IRS 1075 for additional marking requirements for FTI)
Hard Copy	No Label Required	Each page, if loose sheets; front **and** back covers **and** title page, if bound	Each page, if loose sheets; front **and** back covers **and** title page, if bound	Each page, if loose sheets; front **and** back covers **and** title page, if bound
Websites	No Label Required	Internal website only; each page labeled "INTERNAL" on top **and** bottom of page	Internal website only; each page labeled "CONFIDENTIAL" on top **and** bottom of page	Internal website only; each page labeled "RESTRICTED" on top **and** bottom of page

Table 2. Summary of Labeling Requirements

Access Control

Access to Internal or Confidential data may be granted only after a business need has been demonstrated and approved by the Data Steward.

Access to Restricted data may be granted only after a business need has been demonstrated, appropriate training or certification has been provided, and the access is approved by the data owner.

Access Control	Classification			
	Public	Internal	Confidential	Restricted
In-Transit[3]	Basic transport encryption to prevent tampering	• TLS encryption for internal communications	• Strong encryption (TLS 1.2+)	• End-to-end encryption

[3] Authorized users are users that have been granted access to the State of North Carolina Information Systems per the State of North Carolina Statewide Information Security Manual. Restricted information is restricted to authorized individuals who require access to the information as part of their job responsibilities under the principle of least privilege per the State of North Carolina Statewide Information Security Manual. Note: Third party access to federal data may be restricted through federal mandates.

Access Control	Classification			
	Public	Internal	Confidential	Restricted
		• Authentication for internal systems (e.g., SSO, MFA for remote access) • Network segmentation to isolate internal traffic	• Mutual authentication between systems • Strict firewall rules • Data integrity verification	• Enforced MFA and device posture checks • Private network or VPN tunneling • Real-time monitoring and anomaly detection • Network segmentation
At-Rest	Basic file system permissions Integrity checks	• Role-based Access Control • File-level encryption optional but recommended where available for the monitoring of access events	• AES-256 encryption • Roles-based or attribute-based access control • Secure key management • Data masking or tokenization where applicable • Detailed audit logging and alerting	• Full-disk and file-level encryption • Granular ABAC with context-aware policies • Zero-trust architecture principles • Retention and disposal policies • Regular backups • Immutable audit logs • Data loss prevention and automatic redaction • Physical security for storage location

Data Handling for Transfer or Communication

All users must observe the requirements for data handling when transferring or communicating information based on its sensitivity, which are defined in the tables below. Data Stewards, or their assigned representative, may designate additional controls to further restrict access to, or to further protect information.

The following table shows authorized methods for data handling for the transfer or communication of data.

Method of Transfer or Communication	Classification			
	Public	Internal	Confidential	Restricted
Copying	No restrictions	Permission of Data Custodian advised	Permission of Data Custodian required	Permission of the Data Owner required
Fax	No restrictions	Encryption required	Encryption required	Encryption required
Electronic Mail	Encryption optional	External sharing blocked	Encryption required and limited distribution	Encryption required; no printing

Method of Transfer or Communication	Classification			
	Public	Internal	Confidential	Restricted
Spoken Word[4]	No restrictions	Reasonable precautions to prevent inadvertent disclosure	Reasonable measures to ensure that the individual is authorized to receive information; restrict audience as best possible	Active measures to control and limit information disclosure to as few people as possible
Tracking Process by Log	No restrictions	Data Custodian is required to include audit trails for all access and destruction of information	Data Custodian is required to include audit trails for all access and destruction of information	• Data Custodian is required to include audit trails for all access and destruction of information • See IRS 1075 for additional storage requirements for FTI
Granting Access Rights	No restrictions	Data Custodian or designee only	Data Custodian or designee only	Data Owner or designee only
Post (Mail)	No restrictions	Physical access control	Physical access control	• Physical access control • See IRS 1075 for additional storage requirements for FTI
Release to a Third Party	Third party must be an authorized user and have a job-related need[5]	Third party must be an authorized user and have a job-related need[7]	Third party must be an authorized user and have a job-related need[7]	Third party must be a documented and authorized user and have a job-related need[7]

Table 3. Summary of Transfer or Communication Requirements

Media Sanitization

Before disposal or re-use, media must be sanitized in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization*. These methods ensure that data is not unintentionally disclosed to unauthorized users. The baseline for sanitizing media is shown in the table below.

What is Data Sanitization?

Data sanitization is the process of permanently erasing or destroying data from a storage device to ensure it cannot be recovered. It involves the secure and permanent erasure of sensitive data from

[4] Spoken words in the table are defined as transmission by face-to-face conversation, mobile phone, voicemail, and answering machines.
[5] Authorized users are users that have been granted access to the State of North Carolina Information Systems per the State of North Carolina Statewide Information Security Manual. Restricted information is restricted to authorized individuals who require access to the information as part of their job responsibilities under the principle of least privilege per the State of North Carolina Statewide Information Security Manual. Note: Third party access to federal data may be restricted through federal mandates.

datasets and media to guarantee that no residual data can be recovered even through extensive forensic analysis. When data is deleted from storage media, the media is not really erased and can be recovered by an attacker who gains access to the device.

Sanitization	Classification			
	Public	**Internal**	**Confidential**	**Restricted**
	Not required (recommended)	Mandatory	Mandatory	Mandatory

Table 4. Summary of Media Sanitization Requirements

Disposal

Disposing of records must follow all federal and state laws including, but not limited to, the North Carolina Functional Schedule for State Agency, all applicable agency program retention schedules, and in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization.

The following table summarizes disposal methods for the three data classifications. Though there are no specific restrictions on the disposal of low risk data — shredding is generally recommended as a best practice.

Disposal	Classification			
	Public	**Internal**	**Confidential**	**Restricted**
	No restrictions (optional)	Shredding or secure disposal	Shredding or secure disposal	Shredding or secure disposal (certificate of destruction required)

Table 5. Summary of Data Disposal Requirements

Procedural Outlook for Data Disposal – State Agencies & Vendors

Purpose

To ensure the secure and compliant disposal of data that is no longer required for business, legal, or regulatory purposes, in accordance with state policies, data classification, and applicable privacy and security laws.

Roles & Responsibilities

11. **State Agencies:** Responsible for ensuring that internal teams and contracted vendors follow approved data disposal procedures in accordance with this policy and applicable contract terms.
12. **Vendors:** Must comply with state disposal requirements and demonstrate proper destruction practices, especially when handling Confidential and Restricted data.
13. **Security and Privacy Liaisons:** Ensure that disposal aligns with approved sanitization methods.

Disposal Checklist

Once the selected information has been sanitized, each agency and vendor should record the decision and ensure that a process and proper resources are in place to support these decisions.[6]

Documentation

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. The certificate should record at least the following details:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Pre-Sanitization Confidentiality Categorization (optional)
- Sanitization Description (i.e., Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Verification Method (i.e., full, quick sampling, etc.)
- Post-Sanitization Confidentiality Categorization (optional)
- Post-Sanitization Destination (if known)
- For Both Sanitization and Verification:
    - Name of Person
    - Position/Title of Person
    - Date
    - Location
    - Phone or Other Contact Information
    - Signature

Optionally, an organization may choose to record the following (if known):

- Data Backup (i.e., if data was backed up, and if so, where)

A sample “Certification of Sanitization” Form can be found in Appendix G of National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization*.

Aggregation, De-Identification and Commingling

Commingling is defined as the combining of differing data sets rendering them classified, stored, and/or accessed improperly. All attempts must be made to ensure that there is a physical separation of the different data types within the same media. When deemed impossible, the data must be classified and labeled appropriately to the highest classification level with the most stringent security controls implemented.

De-Identified Data is data where all direct or indirect identifiers or codes linking the data to an individual are destroyed or there is no potential for inference-based identification. De-identification can occur by removing the linking identifier or code from the dataset or destroying the linkage file to the point that no

[6] National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization*, p. 19

data can be linked back to an individual. For data subject to HIPAA, de-identification must meet the regulatory requirements set forth by law. De-identified data is classified as “Public.”

Aggregated Data results when data is collected about a group of individuals, de-identified and combined such that no individual can be specific ascertained from the resulting data set. Aggregated data can be used for the purpose of making comparisons or identifying patterns within or among groups of subjects or individuals. Aggregated data would be classified as “Confidential” if the ability to re-identify an individual within the dataset exists.

Exceptions

There are cases where current or future information technology operations cannot achieve compliance with established information technology laws, policies, standards, or practices. In those instances, exceptions may be granted in cases where compensating controls have been applied to reduce risks to an acceptable level. Exceptions to this policy will be handled in accordance with the Statewide Information Security Manual and the Exception Request process. Exceptions will be granted for no longer than one (1) year.

Refer to this link for further information detailing the intended uses of each Exception Request form.

Data Sharing

State agencies that share data must have written agreements that address the business, security and technical requirements regarding the use and custodial responsibilities of the data. These agreements can take the form of a: 1.) Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), Data Use Agreement (DUA) or equivalent contractual agreement, and an Interconnection Security Agreement (ISA) or 2.) a combined agreement.

If the sharing of data is between two state agencies as part of a service, and not otherwise governed by legal requirements, the agencies may choose to use a Service Level Agreement (SLA) that clearly defines the responsibilities, services, priorities and performance metrics of the services to be provided.

Please see the Statewide Data Sharing and Use Procedure.

References

14. 32 CFR Part 2002 CUI Program
15. Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA Administration.
16. Federal CUI Registry
17. FIPS Publication 199 – Standards for Security Categorization of Federal Information and Information Systems, February 2004.
18. H.R. 2458 [Public Law 107-347], 107th U.S. Cong., 2d Sess., E-Government Act of 2002, December 17, 2002.
19. H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., Federal Information Security Management Act of 2002, December 17, 2002.
20. H.R. 3162, Titles VII and Title IX [Public Law 107-56], 107th U.S. Cong., 1t Sess., The USA PATRIOT Act of 2001, October 26, 2001.
21. Health Information Technology for Economical and Clinical Health (HITECH) Act (P.L. 111-5).
22. HIPAA - 45 C.F.R. Part 164 Security and Privacy, and 42 U.S.C.S § 1320d-2 Standards for information transactions and data elements.

23. N.C.G.S. § 14-113.20 – Identity Theft (criminal law).
24. N.C.G.S. Chapter 122C-52 - Right to Confidentiality (relating to health information, N.C. Public Records Act and HIPAA).
25. N.C.G.S. Chapter 126 Article 7 – The Privacy of State Employee Personnel Records.
26. N.C.G.S. Chapter 132 – Public Records Act.
27. N.C.G.S. Chapter 75 Article 2A – Identity Theft Protection Act (civil law).
28. NIST 800-60 – Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories rev 2 Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems (effective August 2008).
29. NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems
30. NIST SP 800-66 Rev. 2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (effective February 2024).
31. NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (effective April 28, 2010).
32. North Carolina General Schedule for State Agency Records established by the Dept. of Cultural Resources.
33. Payment Card Industry (PCI) Data Security Standard – ©2006-2024 PCI Security Standards Council.
34. Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information (effective 2021).
35. S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., Information Technology Management Reform Act of 1996, February 10, 1996.
36. S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., Paperwork Reduction Act of 1995, May 22, 1995.
37. S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., The Privacy Act of 1974, December 31, 1974 (effective September 27, 1975).
38. Social Security Administration Data under the Computer Matching and Privacy Protection Act (CMPPA) of 1988 (Pub. L. No. 100-503) amended the Privacy Act to add several new provisions. See 5 U.S.C. § 552a (a)(8)-(13), (e)(12), (o), (p), (q), (r), (u) (2006).
39. State of North Carolina Statewide Information Security Manual
40. Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA) (2002). United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
41. United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems, Revision 1, February 2006.
42. United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.