NOTE: This policy is effective until March 31, 2026

State of North Carolina

Statewide Data Classification and Handling Policy

N.C. Department of Information Technology

June 2025

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

State Chief Information Security Officer (SCISO).
The Department of Information Technology (DIT) Enterprise Security Risk Management Office (ESRMO).

Scope

This policy applies to all North Carolina state agencies, departments, local governments, institutions, and other entities that are not specifically excluded 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.

Definitions

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

Part 1. Data Classification

Policy

All state data including personal information 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.

Annual Review

This policy, as well as 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.

[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.

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 three-tier system: **1) Low Risk, 2) Medium Risk, or 3) High Risk.** Each is described below.

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 Low Risk and Medium Risk data is classified as Medium Risk.

Data Classification System

Low Risk – Data that is open to public inspection according to state and federal law, or readily available through public sources. Data is classified as Low Risk by default, but agencies are required to explicitly assess and justify this designation, confirming it does not meet the threshold for a higher classification.

Medium Risk (Restricted) – Includes data that, if breached or disclosed to an unauthorized person, is a violation of state or federal law. Medium Risk data and systems may also be referred to as Restricted. The following types of data must be classified as Medium Risk, at a minimum. This is not a complete list and is subject to legislative changes.

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, 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).

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)).

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. 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, are also sensitive public security information.

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 Low Risk.

High Risk (Highly Restricted) – Data that, if breached or disclosed to unauthorized users, has the potential to cause great harm or damage to individuals or institutions. High Risk information can be disclosed only under very specific conditions, if at all. State or federal law or other requirements often include specific standards for protecting High Risk data and systems. High Risk data and systems may also be referred to as Highly Restricted.

- **High Risk data includes the following**:
  State agencies that receive, transmit or store State data classified as personally identifiable information (PII) need to ensure proper safeguards are in place to reduce the probability of unauthorized access and disclosure. Personal identifiable information coupled with other identifying information requires stricter handling requirements because of the increased risk to an individual if the data are compromised.

  Note: Please refer to the Statewide Glossary of Information Technology Terms (SGITT) 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 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 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 DMV 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 (SDCHP). 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 DMV data. Therefore, the State Data Classification and Handling Policy (SDCHP) 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).

The following table summarizes the three data classes.

	Data Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Description	Information not specifically made confidential by State or Federal law.	Information that may be confidential under certain conditions, such as when combined with other data.	Information that can be disclosed under very limited circumstances, if at all.
Types	• Information on publicly accessible websites • Routine correspondence, email and other documents • Work email addresses	• Trade Secrets • Security Features • Sensitive Public Security Information • FERPA • Personal email addresses • Home address	• Personally Identifiable Information • PCI Data Security Standards • PHI/HIPAA • Criminal Justice Information • State and Federal Tax Information • Social Security Administration Provided Information • Attorney-client communications • State Employee Human Resources Records • Driver's information located within NCDMV.

Table 1. Data Classification Summary

Part 2. Data Classification Roles and Responsibilities

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

1. **Data Owner (Data Controller) –** The Agency CIO is the Data Owner for their agency's data except data owned by Federal agencies, the General Assembly, the Judicial Department, and the University of North Carolina (UNC) 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: (1) a system is in place for classifying data, assessing risks, and adequately defining the level of protection for the information which the State collects; (2) proper security measures have been created to support the safeguarding of the State data; (3) oversees the administration of data usage, to ensure compliance with state and federal privacy laws.

2. **Data Steward –** The Office of Privacy and Data Protection are 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 all vendors and agencies are in compliance with state and federal privacy laws.

3. **Data Custodian[2] –** Data Custodians are personnel (e.g., IT & 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 data stewards or their designees, responding to security threats or breaches, and implementing and administering security controls over the information.

4. **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 low, medium and high-risk 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.

5. **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 or breaches immediately.

6. **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. All data subjects have rights under applicable privacy laws, such as access, correction, deletion, notice or restriction of their data.

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.

[2] As used in this policy, the meaning of data custodian is different from G.S. 132-2 and 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."

If known, the applicable statute shall be cited on the label. For example, “Low Risk / Restricted per N.C.G.S. 132-6.1(c)”.

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

Media	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Electronic Media Email/Text Recorded Media CD/DVD/USB (Soft Copy)	No Label Required	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 Physical Enclosure - Label	Creation Date Applicable Statute, if known i.e. “HIGHLY 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
Web Sites	No Label Required	Internal Website Only Each page labeled “RESTRICTED” on top **and** bottom of page	Internal Website Only Each page labeled “HIGHLY RESTRICTED” on top **and** bottom of page

Table 2. Summary of Labeling Requirements

Data Transfer or Communication

All users must observe the requirements for 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.

Access to Low Risk and High-Risk data may be granted only after a business need has been demonstrated and approved by the data steward.

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

Method of Transfer or Communication	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Copying	No Restrictions	Permission of Data Custodian Advised	Permission of Data Custodian Required
Storage	Encryption Optional	• Encryption or physical access control** • No external agency cloud storage***	• Encryption required • No external agency cloud storage***
Fax	No Restrictions	Encryption Required	Encryption Required

Method of Transfer or Communication	Classification		
	Low Risk	Medium Risk (Restricted)	High Risk (Highly Restricted)
Electronic Mail	Encryption Optional	Encryption Required	Encryption Required
Spoken Word*	No Restrictions	Reasonable precautions to prevent inadvertent disclosure	Active measures to control and limit information disclosure to as few persons 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. (See IRS 1075 for additional storage requirements for FTI)
Granting Access Rights	No Restrictions	Data Custodian or Designee Only	Data Custodian or Designee Only
Post (Mail)	No Restrictions	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****	Third party must be an authorized user and have a job-related need****	Third party must be an authorized user and have a job-related need****

Table 3. Summary of Transfer or Communication Requirements

* **Spoken word** in the table is defined as transmission by face-to-face conversation, mobile phone, voice mail, and answering machines.

**Any mobile computing device and portable computing devices such as personal digital assistants (PDAs), smart phones, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct the public's business, must use FIPS 140-2 validated encryption to protect all PII and confidential information, such as personal information, from unauthorized disclosure. It is highly recommended that physical locations with weak access controls, such as satellite offices, deploy full-disk encryption of Restricted and Highly Restricted data.

***Pursuant to N.C.G.S. 143B-1335(b), no external cloud storage is allowed unless explicitly authorized by the State CIO.

****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 per the State of North Carolina Statewide Information Security Manual. Note: Third party access to federal data may be restricted through federal mandates.

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 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		
	Low Risk	Medium Risk (Restricted)	High Risk (Highly Restricted)
	Not required (recommended)	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		
	Low Risk	Medium Risk (Restricted)	High Risk (Highly Restricted)
	No restrictions (optional)	Shredding or secure disposal	Shredding or secure disposal

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 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:

- State Agencies: Responsible for ensuring that internal teams and contracted vendors follow approved data disposal procedures.
- Vendors: Must comply with state disposal requirements and demonstrate proper destruction practices, especially when handling Medium and High Risk data.
- 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.[3]

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 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.

Data aggregation is the process of compiling information from various databases to prepare combined datasets for data processing. If data with different classifications is aggregated, the highest classification must be applied to all the compiled data.

---

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

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.

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.

Appendix. Supplemental Guidance

Classification of Data Not Otherwise Designated by Policy

To classify data not specifically classified by this policy, agencies must conduct an **Impact Analysis** of all data within their respective agencies and use this information to complete a **Privacy Threshold Analysis**. This is a multi-step approach.

- Step 1 – Conduct Impact analysis based on required level of confidentiality, integrity and availability.
- Step 2 – Conduct a Privacy Threshold Analysis of system/data.
- Step 3 – Determine the overall classification of the data and/or system e.g. Low, Medium or High.
- Step 4 – Determine, implement, and test required security controls.
- Step 5 – Perform continuous monitoring of security controls.

State agencies should ensure that the overall classification of the system takes into consideration not only the need for confidentiality based on the type of data, but also the need for availability and integrity. The table below should be used as a reference when determining the impact of loss based on confidentiality, integrity and availability of the data.

Security Objective	Potential Impact		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Confidentiality *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information would have little or no adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, for e.g.: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, i.e. loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
Integrity *Guarding against improper information modification or destruction and includes*	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations,	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational

Security Objective	Potential Impact		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
ensuring information non-repudiation and authenticity.	organizational assets, or individuals.	organizational operations, organizational assets, or individuals.	operations, organizational assets, or individuals.
Availability *Ensuring timely and reliable access to and use of information.*	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Figure 1. Impact Assessment

Additional controls may be required for Medium Risk and High Risk data and systems. The following table provides guidance on data that may require additional controls.

Data Type	Additional Required Security Controls
Health Insurance Portability and Accountability Act (HIPAA)	NIST SP 800-66 Rev. 2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. • Link: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide
Personally Identifiable Information (PII)	NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information. • Link: NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) • Link: DHS Handbook for Safeguarding Sensitive PII
Payment Card Information (PCI)	Information Supplement: PCI DSS Risk Assessment Guideline • Link: PCI Document Library • Link: PCI Risk Assessment Guidelines
Social Security Administration (SSA) Data	Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA Administration. (Provided by SSA upon completion of formal agreement) • Link: Formal agreement between SSA and State Agency
Federal Tax Information (FTI)	Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information • Link: Safeguards for Protecting Federal Tax Returns and Return Information Rev. 2021

References

- Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA Administration.
- FIPS Publication 199 – Standards for Security Categorization of Federal Information and Information Systems, February 2004.
- H.R. 2458 [Public Law 107-347], 107th U.S. Cong., 2d Sess., E-Government Act of 2002, December 17, 2002.
- 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.
- 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.
- Health Information Technology for Economical and Clinical Health (HITECH) Act (P.L. 111-5).
- 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.
- N.C.G.S. § 14-113.20 – Identity Theft (criminal law).
- N.C.G.S. Chapter 122C-52 - Right to Confidentiality (relating to health information, N.C. Public Records Act and HIPAA).
- N.C.G.S. Chapter 126 Article 7 – The Privacy of State Employee Personnel Records.
- N.C.G.S. Chapter 132 – Public Records Act.
- N.C.G.S. Chapter 75 Article 2A – Identity Theft Protection Act (civil law).
- 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).
- NIST SP 800-66 Rev. 2: Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (effective February 2024).
- NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (effective April 28, 2010).
- North Carolina General Schedule for State Agency Records established by the Dept. of Cultural Resources.
- Payment Card Industry (PCI) Data Security Standard – ©2006-2024 PCI Security Standards Council.
- Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies – Safeguards for Protecting Federal Tax Returns and Return Information (effective 2021).
- S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., Information Technology Management Reform Act of 1996, February 10, 1996.
- S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., Paperwork Reduction Act of 1995, May 22, 1995.
- 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).
- 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).
- State of North Carolina Statewide Information Security Manual
- 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.

- 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.
- United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002.