North Carolina Department of Information Technology

Data Classification and Handling Policy

February 2016

CONTENTS

INTRODUCTION

PURPOSE

To create a data classification framework for classifying State data based on the potential harm from the loss, theft or corruption of the information held, processed, transferred or communicated in the course of state business.[1]

OWNER

State Chief Risk Officer

The Department of Information Technology (DIT) Enterprise Security Risk Management Office (ESRMO)

SCOPE

This policy applies to state agencies, departments and other entities not specifically excluded from Article 15 of N.C. General Statute Chapter 143B.

DEFINITIONS

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

PART 1. DATA CLASSIFICATION

POLICY

Information must be maintained in a manner that protects its security and integrity while making it available for authorized use.

Security measures must be implemented commensurate with the potential risk to individuals or institutions from unauthorized disclosure or loss of integrity.

Users of confidential information must observe and maintain the conditions imposed by the providing entity regarding confidentiality, integrity and availability if legally possible.

Annual Review

This policy, as well as all data classifications, must be reviewed at a minimum of 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 data must be classified into one of three classes: 1) Low Risk, 2) Medium Risk, or 3) High Risk. Each is described below.

[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.

The classes determine the level of security that must be placed around the data. The data creator or steward, defined in Part 3 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.

Low Risk – Data that is open to public inspection according to state and federal law, or readily available through public sources.

By default, data is Low Risk unless it meets the requirements 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.

I. **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.

II. **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).

III. **Student Records** – The Federal Educational Rights and Privacy Act (FERPA) generally prohibits the improper disclosure of personally identifiable information derived from education records.

IV. **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 under N.C.G.S 132-6.1(c).

V. **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:

I. **Personal Information and Personally Identifiable Information (PII)** – Under state law, personal information is a person's first name or first initial and last name **in combination** with other identifying information (N.C.G.S. 75-61(10)).

   Identifying information is defined by state law as the following:

   a. Social security or employer taxpayer identification numbers.
   b. Driver's license, state identification card, or passport numbers.
   c. Checking account numbers.
   d. Savings account numbers.
   e. Credit card numbers.
   f. Debit card numbers.
   g. Personal Identification (PIN) Code as defined in N.C.G.S. 14-113.8(6).
   h. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
   i. Digital signatures.
   j. Any other numbers or information that can be used to access a person's financial resources.
   k. Biometric data.
   l. Fingerprints.
   m. Passwords.
   n. Parent's legal surname prior to marriage (N.C.G.S. 14-130.20(b), N.C.G.S. 132-1.10).
   o. Federal law also restricts the use of personal information by state motor vehicle agencies (18 U.S.C. 2721 – Driver's Privacy Protection Act).

II. **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.

III. **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, personally identification numbers, passwords, and card expiration dates.

IV. **Personal 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.

V. **Criminal Justice Information (CJI)** – CJI applies to confidential information from Federal Bureau of Investigation (FBI) Criminal Justice Information Systems (CJIS) provided 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.

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

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 made confidential by State or Federal law. This could include certain conditions such as when combined with other data.	Information made confidential by State or Federal Law that has the potential to cause great harm or damage to individuals or institutions if breached or disclosed to unauthorized users
Types	Information on publicly-accessible websites Routine correspondence, email and other documents	Confidential personnel records Trade Secrets Security Features Sensitive Public Security Information FERPA	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

Table 1 Data Classification Summary

PART 2. SYSTEM CLASSIFICATION

SYSTEM CLASSES

Systems are classified based on the data stored, processed, transferred or communicated by the system and the overall risk of unauthorized disclosure.

The following are the System Classifications:

Low Risk System – Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. Desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Medium Risk or High Risk data.

Low Risk systems must maintain a minimum level of protection as outlined in the State of North Carolina Statewide Information Security Manual, e.g. passwords and data at rest restrictions. Low risk systems are also subject to State laws and may require legal review to ensure that only public data is released in response to a public records request.

Breaches of Low Risk systems can potentially pose significant risk to the State. Websites with high visibility are often targets of opportunities for compromise and defacement. In addition, an unauthorized user may be able to pivot to a higher classified system. However, this policy is confined to data classification requirements.

Medium Risk System – Stores, processes, transfers or communicates Medium Risk data or has a direct dependency on a Medium Risk system. Any system that stores, processes, or transfers or communicates PII is classified as a Medium Risk system, at a minimum.

Highly Risk System – Stores, processes, transfers or communicates High Risk data or has a direct dependency on a High Risk system.

Additional detail about data and system classes can be found in the Appendix under Classification of Data and Systems Not Otherwise Designated by Policy

PART 3. DATA CLASSIFICATION ROLES AND RESPONSIBILITIES

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

I. **Data Owner** – The State CIO is the Data Owner for all state data except data owned by Federal agencies, the General Assembly, the Judicial Department, and the University of North Carolina (UNC) and its constituent institutions.

   Other public officials who have programmatic responsibility for the information contained in records and files must assess risk, classify data and define the level of protection for the information for which they are responsible and may assign data stewards.

II. **Data Steward** – Data stewards are staff with assigned or designated responsibility who have direct operational-level responsibility for information management. Data stewards are responsible for data access and policy implementation issues, and for properly labeling data.

III. **Data Custodian**[2] – Data custodians 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, and implementing and administering controls over the information.

IV. **Data User** – Data users are individuals who need and use data as part of their assigned duties or in fulfillment of assigned roles or functions. Individuals who are given access to medium- and high-risk data have a position of special trust and as such are responsible for protecting the security and integrity of the data.

PART 4. 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.

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.

[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.”

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

Method of Transfer or Communication	Classification		
	Low Risk	Medium Risk (Restricted)	High Risk (Highly Restricted)
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
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 over mobile phone, voice mail, and answering machines as well as face-to-face.

** 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.

DISPOSAL

All disposal of records must follow all federal and state laws including, but not limited to, the North Carolina General Schedule for State Agency Records, any 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 for 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 4 Summary of Data Disposal 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.

Sanitization	**Classification**		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
	Not Required (Recommended)	Mandatory	Mandatory

Table 5 Summary of Media Sanitization Requirements

AGGREGATION AND COMMINGLING

Commingling is defined as differing classification of data resides on the same media. 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 was must be classified and labeled appropriately to the highest classification level with the most stringent security controls implemented.

Data aggregation is the compilation of data. If data with different classifications is aggregated, the highest classification must be applied to all of the compiled data.

EXCEPTIONS

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 DIT Exception Request process.

DATA SHARING

State agencies that share data or systems must have written agreements that address the business, security and technical requirements regarding the use and custodial responsibilities of the data and systems. These agreements can take the form of 1) a 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 or systems 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 AND SYSTEMS NOT OTHERWISE DESIGNATED BY POLICY

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

Step 1 – Conduct a Privacy Threshold Analysis of system/data

Step 2 – Conduct Impact analysis based on required level of confidentiality, integrity and availability.

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 impact of loss based on confidentiality, integrity and availability of the data.

	Potential Impact		
Security Objective	**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, i.e. (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 ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational 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.

Table 6 Impact Analysis

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 Special Publication 800-66: *An Introductory Resource for Implementing the HIPAA Security Rule* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
Personally Identifiable Information (PII)	NIST Special Publication 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf
Payment Card Information (PCI)	Information Supplement: PCI DSS Risk Assessment Guideline https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf
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)
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* http://www.irs.gov/pub/irs-pdf/p1075.pdf

Table 7 – Additional Guidance

REFERENCES

- N.C.G.S. Chapter 132 – Public Records Act
- N.C.G.S. Chapter 75 Article 2A – Identity Theft Protection Act (civil law)
- N.C.G.S. § 14-113.20 – Identity Theft (criminal law)
- N.C.G.S. Chapter 126 Article 7 – The Privacy of State Employee Personnel Records
- N.C.G.S. Chapter 122C-52 - Right to Confidentiality (relating to health information, N.C. Public Records Act and HIPAA)
- North Carolina General Schedule for State Agency Records established by the Dept. of Cultural Resources
- Payment Card Industry (PCI) Data Security Standard – © 2006-2013 PCI Security Standards Council
- HIPAA - 45 C.F.R. Part 164 Security and Privacy, and 42 USCS § 1320d-2 Standards for information transactions and data elements
- Health Information Technology for Economical and Clinical Health (HITECH) Act (P.L. 111-5)
- 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
- NIST 800-60 – Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories rev 1 Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems
- Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA)
- 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).
- S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., Paperwork Reduction Act of 1995, May 22, 1995.
- S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., Information Technology Management Reform Act of 1996, February 10, 1996.
- 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.
- 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.
- 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.
- FIPS Publication 199 – Standards for Security Categorization of Federal Information and Information Systems