DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. This policy covers all State information and information systems to include those used, managed, or operated by a contractor, an agency, or other organization on behalf of the State. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

Responsibilities

All covered personnel involved in the handling of media are responsible for adhering to this policy and with any local maintenance requirements.

Role	Definition
Agency Management	The Agency Head, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level are assigned the responsibility for documenting and implementing data storage media protection practices throughout the agencies.
Agency Security Liaison	The Agency Security Liaison is responsible for ensuring that assigned storage media is managed in compliance with State requirements by collaborating with organizational entities. Liaisons are responsible for maintaining the appropriate operational security posture for agency controlled storage media.
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 in records / 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.
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.
Data Custodian	Data custodians are responsible for providing a secure infrastructure in support of the data, including, but not limited to, providing physical security, back-up 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.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

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.
Information System Owner	The Information System Owner (SO) is responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Third Parties	Third party service providers handling storage media containing sensitive data are responsible for managing storage media in a secure manner, in accordance with this policy.

MP-1 - Policy

All agency information assets must meet the required security controls defined in this policy document that are based on the National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls. This document addresses the requirements set forth by the State to implement the family of Media Protection controls.

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

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

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

Media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, mobile devices including portable storage media such as USB memory sticks and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, tablets, smartphones and cellular telephones digital cameras, and audio recording devices and non-digital media (e.g., paper, microfilm).

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.

The State has adopted the Media Protection security principles established in NIST SP 800-53, “Media Protection” control guidelines as the official policy for this security domain. The “MP” designator identified in each control represents the NIST-specified identifier for the Media Protection control family. The following subsections in this document outline the Media Protection requirements that each agency must implement and maintain in order to protect the privacy and security of sensitive information and to prevent the unauthorized use or misuse of agency data. This policy shall be reviewed annually, at a minimum.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

MP-2 – Media Access

Agencies shall require that access to all digital and non-digital media is restricted to authorized individuals only, using State-defined security measures. Agencies may, at their discretion, restrict the use of removable media in environments that process Highly Restricted data.

a. Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media from unauthorized disclosure and modification throughout the life of those storage media, including disposal.

Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage to data stored on the removable storage media, theft, unauthorized access of data stored on the media, and software licensing violations

b. Assessment of risk must guide the selection of media, and associated information contained on that media requiring restricted access

c. System Owners must document policies and procedures for the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access

d. Document the processes required to ensure the protection of the information of the media and the information on the media from authorized access. This includes, but is not limited to backup media such as tapes or disks or non-digital media

e. Individuals must use only agency approved devices to store Restricted or Highly Restricted data. Personally owned removal devices must not be used on the State Network and for storing non-public data:

    i. All removable media must be encrypted using FIPS 140-2 approved encryption algorithms (e.g. AES 256), unless the Agency CIO or designee has classified the data as public. This includes, but is not limited to devices such as thumb/flash drives, external/removable hard drives, compact disks, magnetic tapes etc.

    ii. All removable devices must be isolated and scanned for malware prior to use on the State Network. Autorun capabilities should be deactivated to reduce any risk of malware leak.

    iii. Any detected malware must be removed from the media. The media must then be verified to ensure that it is safe for use on the State Network.

Using Data Loss Prevention (DLP)

Agencies must use all preventive measure to ensure that the confidentiality, integrity of confidential data remains intact. Data Loss Prevention (DLP) technologies offer automated ways to protect confidential data from being transmitted external to the State Network without being approved and using encryption technologies. Agencies must employ automated tools to monitor internally or at network boundaries for unusual or suspicious transfers or events of the following data types:

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

a. Personally Identifiable Information (PII)

b. Federal Tax Information (FTI)

c. Protected Health Information (PHI)

d. Payment Card Industry (PCI)

e. Criminal Justice Information (CJI)

f. Family Educational Rights and Privacy Act (FERPA)

MP-3 – Media Marking

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

b. 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 technically configurable or it may be done manually.

c. 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)”.

d. Agencies must label removable media (CDs, DVDs, diskettes, magnetic tapes, external hard drives and flash drives) and information system output containing FTI (reports, documents, data files, back-up tapes) indicating “Federal Tax Information”.

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

f. This control is optional for LOW risk information systems.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

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

Data Classification

All data must be classified into one of three classes: 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 **Responsibilitie**s, 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.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

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.

a. **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

b. **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)

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

d. **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)

e. **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:

a. **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

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

other identifying information (N.C.G.S. 75-61(10)): Identifying information is defined by state law as the following:

i. Social security or employer taxpayer identification numbers
ii. Driver's license, state identification card, or passport numbers
iii. Checking account numbers
iv. Savings account numbers
v. Credit card numbers
vi. Debit card numbers
vii. Personal Identification (PIN) Code as defined in N.C.G.S. 14-113.8(6)
viii. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
ix. Digital signatures
x. Any other numbers or information that can be used to access a person's financial resources
xi. Biometric data
xii. Fingerprints
xiii. Passwords
xiv. Parent's legal surname prior to marriage (N.C.G.S. 14-130.20(b), N.C.G.S. 132-1.10)
xv. Federal law also restricts the use of personal information by state motor vehicle agencies (18U.S.C. 2721 – Driver' s Privacy Protection Act)

The following table summarizes the PII and Sensitive PII. **Note:** The table is not exhaustive.

PII includes: Name, email address, home address, telephone number	
Sensitive PII includes the following:	
If stand-alone	***If paired with the above identifiers***
Social Security Number (SSN)	Citizenship or immigration status
Employer taxpayer identification numbers	Position description and performance plans without ratings
Driver's license or State ID #	Medical information
Passport Number	Ethnic or religious affiliation
Alien Registration Number	Sexual orientation
Financial account numbers (banking, credit, debit, etc.), or any other numbers or information that can be used to access a person's financial resources.	Account passwords

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

Biometric identifiers	Last 4 digits of SSN
Personal Identification (PIN) Code as defined in N.C.G.S. 14-113.8(6).	Date of birth
Digital signatures	Criminal history
Biometric data.	Mother's maiden name
Fingerprints	Electronic identification numbers
Passwords	Internet account numbers, or Internet identification names

b. **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. Federal tax information is defined in IRC 6103 (b)(1).

c. **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

d. **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

e. **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. Criminal Justice Information is defined in the Criminal Justice Information Services (CJIS) Security Policy.

f. **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 as identified in paragraph (a) under **High Risk (Highly Restricted)**.

The following table summarizes the three data classes, Low Risk, Medium Risk (Restricted), and High Risk (Highly Restricted).

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

	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

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.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

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.

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

MP-4 - Media Storage

Agencies shall ensure the proper storage of data and information files for which they are responsible.

a. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse.

b. Agencies shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.

c. Agencies shall protect the State's information and comply with the agency records retention policy or the General Schedule for State Agency Records, Information Technology Records.

d. Agencies shall ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, agencies shall follow the statewide information security standard for encryption.

e. Agencies shall establish change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures.

f. All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.

g. Agencies shall physically control and securely store media containing FTI.

h. Agencies shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

i. Agencies shall encrypt data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices, i.e. backups) as required for the protection of the highest level of information contained therein.

j. Agencies shall keep stored public data to a minimum of what is necessary to adequately perform their business functions. Sensitive or confidential data that is not needed for normal business functions, such as the full contents of a credit card magnetic strip or a credit card PIN, should not be stored. Agencies should consider implementing a process (automatic or manual) to remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the agency's data retention policy.

k. This control is optional for LOW risk information systems.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

Media Archival

Agencies shall consult with the NC Department of Natural and Cultural Resources, Government Records Section, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived. In addition, the following requirements must be met:

a. When archiving data associated with legacy systems, agencies should plan to provide a method of accessing those data.

b. Classification of the back-up media so the sensitivity of the data can be determined.

c. Storage of media back-ups in a secure location, preferably an off-site facility.

d. All back-up media are physically secured from theft and destruction.

e. Migrating data to another system or archiving data shall be in accordance with applicable records management regulations and policies for potential future access.

MP- 5 – Media Transport

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 representatives, may designate additional controls to further restrict access to, or to further protect, information:

a. Access to data shall be granted only after a business need has been demonstrated and approved by the data steward.

b. Agencies must use transmittals or an equivalent documented tracking method to ensure FTI and other Restricted or Highly Restricted data reaches its intended destination.

c. Media are transported by secured courier or other delivery method that can be accurately tracked.

d. Management approval shall be obtained before moving any media from a secure area.

e. Inventory logs of all media shall be properly maintained, and an inventory of all media logs, shall be performed at least annually.

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

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

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****

* 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 that is stored on the device 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.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

*** 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.

MP-6 – 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 data is not unintentionally disclosed to unauthorized users. Media containing Highly Restricted data shall be sanitized prior to disposal, release out of agency control, or release for reuse using agency approved sanitization techniques in accordance with applicable federal and agency standards and policies. 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

Media Disposal

Agencies shall protect data confidentiality and integrity through proper disposal of obsolete equipment and protect information by using secure software disposal techniques.

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.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

Disposal	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk**
	No restrictions (Optional)	Shredding, degaussing or secure disposal	Shredding, degaussing or secure disposal

MP-7 – Media Use

State and agencies shall ensure that security controls are in place to protect the confidentiality and integrity of the State's data stored on information system storage media throughout the life of those storage media, including disposal:

a. Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage to data stored on the removable storage media, theft, unauthorized access of data stored on the media and software licensing violations.

b. Prohibit the connection of any non-State or agency owned information system data storage media, mobile device or computers to a State-owned resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.

c. The use of sanitization-resistance media that does not support sanitization commands, or if supported, the interfaces are not supported in a standardized way across these devices is prohibited for use with Highly Restricted data. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.

d. Acceptable Use Policies (AUPs) shall define the proper use of information assets and shall include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage and Internet usage.

Aggregation and Commingling

Commingling of differing classifications of data on the same media must be prohibited. 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.

When data with different classifications is gathered and summarized; and thus aggregated, the highest classification must be applied to all the aggregated data.

DocuSign Envelope ID: 47E92340-69A8-41E6-ACF5-32E9F690D504

MP-7 (1) – Media Use – Prohibit Use Without Owner (Moderate Control)

Agencies shall prohibit the use of portable storage devices in State information systems when such devices have no identifiable owner. Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., malicious code insertion).

MP-8 – Media Downgrading (Optional Control)

This control is optional for LOW and MODERATE risk information systems.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Material Superseded

This current policy supersedes all previous versions of the policy. All State agencies and vendors of the State are expected to comply with the current implemented version of this policy.

Approved: DocuSigned by: Tracy Doaks EEADAC04EB804A3... 3/3/2020 | 11:17 AM EST

Secretary of Department of Information Technology (DIT)