GOVERNANCE

This document is governed by the IT Governance policy which provides the following guidance:

a. Roles and Responsibilities
b. Policy Control Application
c. Policy Compliance Requirements
d. Policy Exceptions and Exemptions
e. Policy Reviews and Updates

SCOPE

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.

MP-1 POLICY AND PROCEDURES

All information assets that process, store, receive, transmit or otherwise impact the confidentiality, integrity, and accessibility of State data must meet the security controls defined in this policy based on the National Institute of Standards and Technology (NIST) SP 800-53 r5, Security and Privacy Controls. A designator followed by a number in parenthesis indicates a control enhancement that provides statements of security and privacy capability that augment a base control. Only those control enhancements associated with the moderate level controls are listed. Should an executive-branch agency be required to address other control enhancements for a control item, the organization will be responsible for writing an additional policy to meet that requirement.

This document addresses the requirements set forth by the State for the family of Media Protection controls at the organization, process and/or system level for all State data and information assets.

a. Information must be maintained to protect its security, integrity, and availability for authorized use.
b. Security measures shall be implemented commensurate with the risk to the State from unauthorized disclosure or integrity loss.
c. Users of sensitive or confidential information must observe and maintain the conditions imposed by the State regarding confidentiality, integrity, and availability if legally possible.

Media includes, but is not limited to, digital media such as diskettes, magnetic tapes, external/removable hard drives, memory sticks, and portable computing devices, including:

- Notebook/laptop computers
- Tablets, such as iPads, Surface, and similar
- Smartboards
- Smart/cellular phones
- Video recording devices
- Audio recording devices
- Drones

Media also includes, but is not limited to, printed information, hand-written notes with sensitive or confidential information, microfilm, and microfiche.

Data classifications must be reviewed at least annually or when a State-defined event impacting the data/system security posture occurs. This includes but is not limited to:

- Commingling of data with different risk/classification levels.
- Data decoupling.
- Interconnecting high-risk systems with systems of lower risk classifications.

For all media types, the following security requirements shall be considered:

- Security controls shall be implemented to protect the confidentiality and integrity of data on removable storage media from unauthorized disclosure and modification for its complete lifecycle - including disposal.
- All removable media shall be encrypted using the latest FIPS 140 validated encryption algorithms.
- Individuals shall use only State-approved or supplied devices to store sensitive or confidential data; and personally owned removable devices shall not be used in State information systems, or for storing non-public data.
- All removable devices shall be isolated and scanned for malicious code prior to State information systems introduction. Autorun capabilities should be deactivated. Any detected malware or equivalent shall be removed from the media, which must then be verified to ensure it is safe for State use.
- Use of removable or portable storage devices without an identifiable owner is prohibited on State systems.
- Risk assessments shall guide the selection of media and the risk level of data stored thereon.
- Data Loss Prevention (DLP) technology shall be used to monitor internal and network boundaries for suspicious or unusual data transfers or events including but not limited to:
    1. PII – Personally Identifiable Information
    2. FTI – Federal Tax Identifiable Information
    3. PHI – Protected Health Information
    4. PCI – Payment Card Industry
    5. CJI – Criminal Justice Information

This policy and associated procedures shall be reviewed and updated at least every three (3) years, or when State-defined events occur that require off-cycle review/updates.

MP-2 MEDIA ACCESS

Access to all State-owned media classified as Internal, Sensitive, or Confidential shall be restricted to authorized individuals only.

Access controls shall include physical protection and accountability for removable media to minimize the risk of device theft, and protect the confidentiality, integrity, and availability of stored data.

System Owners shall document policies and procedures for any media containing sensitive or confidential data to restrict access to only authorized individuals, and the specific measures used to

restrict access.

MP-3 MEDIA MARKING

System media containing sensitive or confidential Information shall be marked with human readable information regarding the access/distribution parameters/permissions and handling requirements based on the classification level(s) of the data contained. System media marking shall reflect applicable laws, orders, directives, policies, standards, and guidelines.

MP-4 MEDIA STORAGE

Stored data and information shall be physically controlled and digitally secured as described below:

a. Stored data shall be protected and backed up to facilitate restoration from accidental or unauthorized deletion or misuse.
b. All applicable statutory and regulatory requirements for data retention, destruction, and protection shall be met.
c. Organizations shall protect State information and comply with the organization's records retention policy.
d. Encryption keys shall be separately and securely stored and available for decryption. When using encryption to protect data, the State's information security standard for encryption shall be followed at a minimum.
e. Change management procedures shall be established for emergency amendment of data that occurs outside normal software functions and procedures.
f. All emergency amendments or changes shall be properly documented and approved to meet statutory and regulatory requirements.
g. Information system media shall be protected until the media is destroyed or sanitized using approved equipment, techniques, and procedures.
h. Data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices, e.g., backups) shall be encrypted as required for the protection of the highest level of information contained.
i. Stored public data shall be kept to a minimum to adequately perform their business functions. Sensitive or confidential data 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.

MP-5 MEDIA TRANSPORT

All users of State system media shall protect and control sensitive and confidential data based on its sensitivity when transferring or communicating this information.

a. Access to data shall be granted only after a business need has been demonstrated and approved by the data steward.
b. Transmittals or an equivalent documented tracking method must be used to ensure sensitive or confidential data reaches its intended destination.
c. Media is transported by secure courier or other accurately trackable delivery method.
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.

MP-6 MEDIA SANITATION

The State shall sanitize media before disposal or re-use to ensure sensitive or confidential data is not disclosed to unauthorized users.

Media shall be sanitized to National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization* protocol. Media containing confidential data shall be sanitized prior to disposal, released from agency control, or for reuse using agency approved sanitization techniques.

Sanitization is required for any sensitive or confidential information and is recommended but not required for information at lower classification levels.

Media Disposal:

- Data confidentiality and integrity shall be protected through proper disposal of obsolete equipment and by using secure software disposal techniques.
- All disposal of records must follow all federal and state laws, any agency program retention schedules, and as required to meet with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, Guidelines for Media Sanitization.

MP-7 MEDIA USE

The State shall implement security controls to protect the confidentiality and integrity of the sensitive and confidential data stored on information system storage media throughout the storage media lifecycle including disposal.

The State shall:

a. Ensure access control of/to media including but not limited to physical protection of and accountability for removable media to minimize the risk of theft, unauthorized access, and software license issues.
b. Prohibit the connection of any non-State-owned information system data storage media, mobile device, or computers to a state resource, unless connecting to a guest network or guest resources. This requirement may be contractually circumvented at State or executive-branch agency discretion for approved vendors providing operational IT support services.
c. Prohibit the use of portable storage devices in agency systems when such devices have no identifiable owner.
d. Prohibit the use of sanitization-resistance media that does not support sanitization commands containing sensitive or confidential data. Sanitization-resistant media include, for example, compact flash, embedded flash on boards and devices, solid state drives, and USB removable media.
e. Define the proper use of information assets and include items such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage, and internet usage.

f. Prohibit commingling different data classifications on the same media. If commingling is unavoidable, then the data must be classified and labeled to the highest classification contained.

MP-7 (1) MEDIA USE – PROHIBIT USE WITHOUT OWNER

The State shall prohibit the use of portable storage devices with no identifiable owner. Requiring identifiable owners for portable storage devices reduces risk by assigning responsibility and accountability for addressing known device vulnerabilities.

POLICY OWNER

Secretary of Office of Information Technology (OIT)

MATERIAL SUPERSEDED

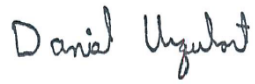
This current policy supersedes all previous versions, and all State agencies and vendors of the State are expected to comply with the current implemented version.

REVISION HISTORY

Revision Date	Summary of Change
12/31/2024	Policy Update

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK

APPROVED BY

Signature	
Approved by	Daniel Urquhart
Title	Secretary of Office of Information Technology (OIT)
Date Approved	01/15/2025

REMAINDER OF PAGE LEFT INTENTIONALLY BLANK