State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
OMIS Policy #0539: Media Protection

Revised: February 10, 2025

1.0 PURPOSE

The WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and the Office of Shared Administration (OSA), Office of Management Information Services (OMIS) will protect the Departments' data against information loss by ensuring all data is protected from unauthorized disclosure. Each bureau and office, as data owner(s), must follow federal, state, and OMIS security controls to ensure both digital and non-digital media containing restricted and/or sensitive data {i.e., protected health information (PHI), personally identifiable information (PII), federal tax information (FTI), payment card information (PCI), and social security administration (SSA) data} is controlled, tracked, securely stored, and properly disposed of.

This policy will provide the Departments with methods to properly manage all digital and non-digital media and to minimize the risk of confidential data loss, unauthorized disclosure, or loss of integrity resulting in a possible data breach. To protect information assets, all bureaus and offices must utilize the baseline controls and standards established by NIST Special Publication (SP) 800-53, *Security and Privacy Controls*, to categorize assets.

2.0 SCOPE

This policy applies to all DH, DHF, DoHS, and OSA employees and authorized system users, which includes, but is not limited to county offices, state hospitals, local health departments, boards and commissions, business associates, contractors, and vendors as they fall within the authorization to access resources granted by the State.

This policy applies to all IT environments and assets owned or operated by the State or an authorized vendor. Bureaus and offices under the policy authority, but not under the direct management of OMIS, must independently comply with the requirements of this policy.

For this policy, "information systems media" means any state-owned media, which includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, mobile devices including portable storage media such as USB drives, and portable computing and communications devices with storage capability, i.e., notebook/laptop computers, tablets, smartphones and cellular

telephones, digital cameras, and audio recording devices) as well as non-digital media (e.g., paper, microfilm).

3.0 POLICY

3.1 All State and Department information assets must meet the required security controls as defined in the NIST SP 800-53 (for more information on NIST controls see Section 6.0 of this policy). This document addresses the policies and standards set forth by the State to implement the family of Media Protection controls for all information assets and data at the Department, process, and/or system level.

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

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

3.1.3 Users of confidential information must observe and maintain the conditions outlined by the Executive Branch and the Departments regarding confidentiality, integrity, and availability if legally possible.

3.2 All DH, DHF, DoHS, and OSA employees must adhere to the standards outlined in WVOT-PO1011 – *Digital Media Protection.*

3.3 Users are accountable for protecting restricted and/or sensitive data on portable and writable media.

3.4 Network controls will be implemented to limit access to portable media devices (e.g., USB drives).

3.4.1 Employees must not use portable media to transfer restricted and/or sensitive data if an alternate electronic means of secure file transfer is or can be made reasonably available (i.e., SFTP, FTPS, etc.).

3.4.2 All DH, DHF, DoHS, and OSA employees must complete a Privacy Impact Assessment (PIA) prior to purchasing either a USB drive or an external hard drive. If the media will store PII, a risk assessment may be required. (See the following link for more information: https://privacy.wv.gov/privacyimpactassessment/Pages/default.aspx.)

3.4.2.1 If the data on the removable media contains PHI, PII, or other protected data, the removable media must be encrypted using Industry-standard, well-tested encryption algorithms. See Section 3.13 of this policy for additional information.

3.4.3 Employees must not uninstall or de-activate any security controls loaded onto media devices by the WVOT, or its designee.

3.4.4 System administrators may use group policies, security templates, and other controls to disable portable media capabilities and ensure monitoring capabilities are present to detect changes in account permissions.

3.4.5 The OMIS Chief Information Officer (CIO) may prohibit flash drive use at any time to protect data. This prohibition should be implemented through policy, training, and/or use of technical controls (e.g., port blocking control).

3.4.6 The WVOT will establish audit trails or logs in all situations it deems is warranted. The resulting records will allow tracking of the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The WVOT has the right

to monitor all employee access and/or connection to the State network to identify and analyze unusual usage patterns or other activity.

3.5 Media Management

3.5.1 The WVOT will establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive and/or restricted data on digital and non-digital media.

3.5.2 OMIS will work with DH, DHF, DoHS and the OSA bureaus and offices to assign a data custodian(s) for all media containing sensitive and/or restricted information. The data custodian(s) will ensure the media is protected at the level required by its classification (see WVOT-PO1006, *Data Classification*).

3.5.3 The data custodian(s) must ensure control and accountability of sensitive and/or restricted information on the media he/she manages. This includes maintaining accurate inventory and disposal records, as well as monitoring the media while in use and when it is no longer associated with the system.

3.6 Media Access (MP-2)

3.6.1 Access to data will be granted only after a business need has been demonstrated and approved by the data owner.

3.6.2 Access controls must include physical protection of and accountability for removable media to minimize the risk of theft, software licensing violations, as well as unauthorized access and/or damage to data stored on the media.

3.6.3 System Owners must keep a record of any media requiring restricted access, all individuals authorized to access the media, and the specific measures taken to restrict access.

3.6.4 All employees must protect electronic and physical media containing restricted and/or sensitive data while at rest, stored, or actively being accessed. Employees are prohibited from using flash drives or portable media that do not have adequate protection mechanisms to store or transmit sensitive data (e.g., PHI, PII, FTI, SSA data). For more information see WVOT-PO1011, *Digital Media Protection*.

3.6.5 Employees must not use publicly accessible devices to access, process, store, or transmit sensitive and/or restricted data. Publicly accessible devices are PCs that may be in hotel business centers, convention centers, public libraries, public kiosks, etc.

3.6.6 Precautions must be taken to obscure sensitive and/or restricted data from public view, (i.e., using session lock and/or privacy screens on laptops).

3.6.7 Employees must use only WVOT-approved devices to store sensitive and/or restricted data. Employees must not use personally owned devices to access, process, store, or transmit data.

3.6.8 Access to media containing restricted and/or sensitive data must be physically restricted to authorized personnel.

3.7 Data Loss Prevention

3.7.1 System owners must use preventive measures to ensure the confidentiality and integrity of sensitive and/or restricted data remains intact. Data Loss Prevention (DLP) technologies offer automated ways to protect confidential data from being transmitted to a location external to the State network without being approved and without using encryption technologies.

3.7.2 System owners will employ automated tools to monitor internally or at network boundaries for unusual or suspicious transfers or events of the following data types:

(a) PII;
(b) FTI;
(c) PHI;
(d) PCI data;
(e) SSA data; and
(f) Others as necessary

3.8 Media Marking (MP-3)

3.8.1 All media containing PII, PHI, FTI, PCI, or SSA data must be appropriately marked and labeled to indicate the sensitivity of the data (see WVOT-PO1006 – *Data Classification* for more information). Data owners within the Departments must appropriately label information system media to indicate the following:

(a) If it contains sensitive and/or restricted information.
(b) The classification of the data (i.e., restricted, sensitive, etc.).
(c) The distribution limitations of the information.
(d) Handling requirements according to data classification, risk potential, etc.
(e) Other applicable security markings (if any).

3.8.2 If marking the media itself is not practicable, the data owner must mark the container appropriately. If known, the applicable statute or policy may be cited on the label. (For example, "Low Risk/Restricted per WVOT-PO1006 – *Data Classification*.)

3.8.2.1 Recipients of the media must maintain the assigned marking and protect the information.

3.8.2.2 Data owners must label removable media and information system output containing FTI (i.e., reports, documents, data files, back-up tapes) indicating "Federal Tax Information".

3.8.2.3 Specific types of media or hardware components remaining within a secure environment may be exempted from marking if approved, in writing, by the OMIS CIO or a designee.

3.8.3 Marking information system media must reflect applicable state and federal laws, Executive Orders, and Executive Branch and OMIS policies and standards.

3.8.4 Security marking is generally not required for media containing information determined by the data owner to be in the public domain or to be publicly releasable. However, the data owner may require marking for public information indicating that it is publicly releasable.

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

MEDIA	**Classification**		
	Low Risk	**Medium Risk**	**High Risk**
Electronic Media Email/Text Recorded Media CD/DVD/USB (Soft Copy)	No Label Required	Creation Date Applicable Statute, if known i.e. "RESTRICTED per WVOT-PO1006 External **and** Internal labels	Creation Date Applicable Statute, if known i.e. "HIGHLY RESTRICTED per WVOT-PO1006 External **and** Internal labels

		Email – Beginning of Subject Line Physical Enclosure - Label	Email – Beginning of Subject Line (See IRS Pub.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

3.9 Data Classification

3.9.1 Access will be controlled using appropriate security measures based on the characteristics of the information including, but not limited to, the classification of the information.

3.9.2 Commingling of different classifications of data on the same media is prohibited. All attempts must be made to ensure that physical separation of the different data types occurs within the same media. When separation is impossible, the data must be classified and the highest classification must be applied.

3.9.3 Data owned or maintained by Departments will be put into appropriate classification levels, according to its sensitivity and criticality. Levels include **Public (low risk), Sensitive (medium risk), and Restricted (high**

risk). For more information see WVOT-PO1006, *Data Classification*. The following table summarizes the three data classes:

	Data Classification		
	Public Low Risk	**Sensitive Medium Risk**	**Restricted High Risk**
Description	This data is open and public with no distribution limitations. It is published and distributed freely, without restriction.	This data is made available through open record requests or other legal processes. Access is limited to authorized individuals who require access to the information to perform their job duties.	This is the most sensitive data and has the most stringent security controls. Access to this data is protected by state and federal regulations and is limited to authorized individuals.
Types	Examples include but are not limited to occupational licensing data excluding SSNs, public-facing websites, policies and procedures, etc.	Examples include but are not limited to employee records, operational and inventory information, state or federal contracts data, etc.	Examples include, but are not limited to social security numbers, foster care data, PHI, PII, federal tax information FTI, etc.

3.9.4 System Classes: Systems are classified based on the data stored, processed, transferred, or communicated by the system and the overall risk of unauthorized disclosure. Types of systems include low, medium, and high risk.

3.9.4.1 Low Risk Systems

a. Low risk systems only contain data that is public by law or directly available to the public via such methods as the Internet. State-provided desktops, laptops, and supporting systems are low risk unless they store, process, transfer, or communicate medium or high-risk data.

b. Low risk systems must maintain a minimum level of protection as outlined in Executive Branch and OMIS information security policies and standards.

c. Low risk systems are subject to State laws and WV State Privacy Office privacy policies and may require legal review to ensure that only public data is released in response to a public records request.

3.9.4.2 Medium Risk Systems

a. Medium risk systems store, process, transfer, or communicate medium risk data or have 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.

3.9.4.3 High Risk Systems

a. High risk systems store, process, transfer, or communicate high risk data or have a direct dependency on a high-risk system.

3.9.5 All data classifications must be reviewed annually, at a minimum, or when a significant change exists 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 (see WVOT-PO1015 – Change Management policy).

3.10 Media Storage (MP-4)

3.10.1 Employees may not use removable media devices for primary or long-term data storage. Removable media may be used for short-term data storage and backup purposes if the State network connection is unavailable (e.g., offsite use). If data is not currently in use, or if critical data may be needed for an extended period, users may utilize offline storage. For additional information, see WVOT-PO1011, *Digital Media Protection* policy, or contact the WVOT.

3.10.2 DH, DHF, DoHS and OSA bureaus and offices must ensure the proper storage of data and information files (both digital and non-digital) for which they are responsible. Secure storage for non-digital data includes locked drawers, desks or cabinets, and/or a controlled media library. Employees must adhere to the following guidelines:

(a) Employees must guard against access to data and take precautions to protect IT devices when away from the workstation. This includes, but may not be limited to, logging off or locking the computing device; ensuring monitors are positioned away from view, when possible; and storing sensitive, restricted, and essential data on a cloud-based file storage service (e.g., G drive) rather than on the computing devices' internal hard drives.

(b) Stored data must be protected and backed up so restoration can occur in the event of accidental or unauthorized deletion or misuse.

(c) Employees must protect the State's information and comply with the Departments' records retention policy. (See the *Records Retention and Disposal Schedule policy at the following link*: http://intranet.wvdhhr.org/policies/Policies/Records%20Retention%20Schedule%209-30-16.pdf).

(d) Employees must ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, employees must follow NIST SP 800-53 standards .

(e) Minimum protection standards (MPS) establish a standardized method for physically protecting data, systems, and non-electronic forms of FTI. MPS requires a minimum of two layers of security to access FTI and will be applied on a case-by-case basis (e.g., physical copies of FTI must be stored in a locked cabinet within another locked room or office).

(f) All Executive Branch employees must protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures. (This process is outlined in West Virginia Code §5A-6-4, *Procedures for Sanitization, Retirement and Disposition of Information Technology Equipment*).

(g) Sensitive and/or restricted data stored on secondary storage devices (i.e. backups) must be encrypted, as required, by CP-9 in NIST SP 800-53 for the protection of the highest level of information contained therein.

(h) Bureaus and offices must maintain stored public data to a minimum of what is necessary to adequately perform business functions. If sensitive and/or restricted data is not needed for normal business functions, (i.e.,

full contents of a credit card magnetic strip or a credit card PIN), it should not be stored.

3.10.4 When receiving, processing, storing, or transmitting sensitive and/or restricted data, the system owner must enforce physical access authorizations at entry/exit points to facilities where the information systems reside by:

1. Verifying individual access authorizations before granting access to the facility.
2. Controlling entry/exit to the facility using physical access control systems/devices or guards. This may include:

   a. Maintaining physical access audit logs for entry/exit points.
   b. Providing security safeguards to control access to areas within the facility officially designated as publicly accessible.
   c. Escorting visitors and monitoring visitor activity.
   d. Securing keys, combinations, and other physical access devices.
   e. Maintaining an inventory of physical access devices (i.e., keys, locks, combinations, and card readers).
   f. Changing combinations and keys at least annually, or when an employee retires, terminates employment, or transfers to another position.

3.11 Media Archival

3.11.1 Departments must work with WVOT to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived. The following requirements must be met:

(a) When archiving data associated with legacy systems, system owners must provide a method of accessing those data.

(b) Classification must be given to the backup media so the sensitivity of the data may be determined.

(c) Back-up media must be physically secured from theft and destruction and stored in a secure location, preferably an off-site facility.

(d) Data owners must ensure compliance with applicable records management regulations and policies related to potential future access when either archiving data or migrating data to another system.

3.12 Media Transport (MP-5)

3.12.1 All users must observe the requirements for transferring or communicating information based on its sensitivity. Data owners, or their designees, may assign additional controls to further restrict access to, or to further protect, information.

3.12.3 Transmittals or an equivalent documented tracking method must be used to ensure FTI, and other sensitive or restricted data reaches its intended destination.

3.12.4 Data custodians will maintain inventory logs of all media, which must be reviewed at least annually.

3.12.5 To prevent inadvertent or inappropriate disclosure and use while in transport outside a controlled area, data owners must establish controls to protect both digital and non-digital media that could contain restricted and/or sensitive data.

3.12.6 An identified data custodian must be used during the transport of all information system media containing sensitive and/or restricted data,

ensuring the pickup, receipt, transfer, and delivery of such media is restricted to authorized personnel.

3.12.7 Dissemination to individuals outside controlled areas is only authorized under the following conditions:

1. The external organization/individual is an authorized recipient of such information and is being serviced by the accessing organization.
2. The data custodian must maintain accountability for information system media during transport.
3. The data custodian must verify all activity associated with the transport of information system media.
4. The data owner must ensure any digital media containing PII, PHI, FTI, SSA, and/or PCI data is encrypted using FIPS-validated encryption during transport.
5. Neither data owners nor custodians will take confidential data from a secure area unless authorized by management.

3.12.8 The Departments' data custodians will control, protect, and secure digital and non-digital media from public disclosure during transport by:

1. Using cryptography and tamper-evident packaging.
2. Requiring confidentiality statements for digital and non-digital media, if applicable.
2. Limiting the collection, disclosure, sharing, and use of sensitive and/or restricted data.
3. Following least privilege and role-based rules for allowing access.
4. Securing hand-carried confidential electronic and paper documents by:

   a. Only viewing or accessing sensitive and/or restricted data electronically or via document printouts in a physically secure location approved by authorized personnel.

b. Handling hard copy documents with the following standards:

i. Package hard copy printouts in such a way that no sensitive and/or restricted information is viewable.

ii. When sensitive and/or restricted data is mailed or shipped, employees must use an opaque file folder or envelope for hard copy printouts, use a delivery method in which the data can be accurately tracked, and only release the data to authorized individuals.

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

Method of Transfer or Communication	**Classification**		
	Low Risk (Public)	**Medium Risk (Sensitive)**	**High Risk (Restricted)**
Copying	No Restrictions	Permission of Data Custodian Advised	Permission of Data Custodian Required
Storage	Encryption Optional	Encryption or physical access control** No external cloud storage***	Encryption required No external cloud storage***
Fax	No Restrictions	Encryption Required	Encryption Required
Electronic Mail	Encryption Optional	Encryption Required	Encryption Required
Spoken Word*	No Restrictions	Reasonable precautions to	Active measures to control and limit

		prevent inadvertent disclosure	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 Pub 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 Pub 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 face-to-face conversations.

** 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 USB drives that are used to conduct the public's business, must use FIPS 140-2 validated encryption to protect all PII and confidential information

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 data.

*** Cloud computing services used to receive, transmit, store, and process State data must be vetted and approved by the WVOT Chief Information Technology Officer and the Chief Information Security Officer. All Executive Branch employees must follow the requirements in Section 3.5 in WVOT-PO1006, Data Classification.

**** Authorized users are users that have been granted access to the Executive Branch information systems by WVOT (see WVOT-PO1021, Account Management). Restricted information is restricted to authorized individuals who require access to the information as part of their job responsibilities. Note: Third party access to federal data may be restricted through federal mandates.

3.13 Encryption Protection (MP-5(4))

3.13.1 All media must be encrypted with WVOT-approved software, where technically possible, 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.

3.13.2 When sensitive data is at rest (i.e., stored electronically) outside the boundary of the physically secure location, the data must be encrypted to protect the confidentiality and integrity of the information.

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

3.14 Media Sanitation, Destruction, and Disposal (MP-6)

3.14.1 Before disposal, release from Departments' control, or release for reuse, all digital and non-digital media must be sanitized and destroyed using

defined techniques and procedures in accordance with applicable NIST controls, WV Code, and Executive Branch policy.

3.14.2 West Virginia Code §5A-6-4, *Procedures for Sanitization, Retirement, and Disposition of Information Technology Equipment*, requires that technology equipment be disposed of by the WVOT, using Federal Information Processing Standards (FIPS)-validated media sanitization techniques.

3.14.3 All digital media will be sanitized utilizing mechanisms appropriate to the security category or classification of the information. Sanitation methods must conform to state and federal records retention policies.

3.14.4 WVOT will document, verify, and maintain the steps taken to sanitize or destroy digital and non-digital media and ensure that authorized personnel witness or carry out the sanitization or destruction.

3.14.4.1 Digital media sanitation methods must agree with NIST SP 800-88 revision 1, *Guidelines for Media Sanitation*.

3.14.4.2 Non-digital media must be finely shredded using approved equipment, techniques, and procedures, with a minimum of cross-cut shredding.

3.14.5 WVOT will exercise proper control of confidential information to avoid data leakage due to improper disposal of storage media or improperly wiped refurbished media. Sanitation methods must be consistent with NIST SP 800-88 Guidelines.

3.14.6 WVOT is responsible for testing sanitization equipment and procedures annually to verify that the intended sanitization is being achieved.

3.14.7 WVOT will track and document the following: (a) personnel who reviewed and approved sanitization and disposal actions; (b) the types of media sanitized; (c) specific files stored on the media; (d) the sanitization methods used; (e) the date and time of the sanitization actions; (f) the personnel performing the sanitization; (g) any verification actions taken; (h) and the disposal action taken. WV Surplus Property will verify that the sanitization of the media was effective prior to disposal.

3.14.8 Non-destructive sanitization techniques will be applied to portable storage devices before connecting to State systems and/or equipment under the following circumstances: (a) prior to initial use after purchase; (b) when obtained from an unknown source; (c) when the organization loses a positive chain of custody; (d) and when the device was connected to a lower assurance network/system (e.g., based on FIPS 199 security categorizations).

3.14.9 Physical media will be securely disposed of at end-of-life, per NIST SP 800-88, revision 1, and using approved equipment, techniques, and procedures. For more information, refer to **WV State Code §5A-6-4(14)**.

3.15 Media Use (MP-7)

3.15.1 Security controls will be in place to protect the confidentiality and integrity of all DH, DHF, DoHS, and OSA data stored on information system storage media throughout the life of those storage media, including disposal.

3.15.2 Employees will not connect any non-State-owned information system data storage media, mobile device, or computer to a State-owned resource, unless authorized by OMIS or WVOT.

3.15.3 OMIS prohibits the use of portable storage devices in State information systems when such devices have no identifiable owner.

3.15.4 All DH, DHF, DoHS, and OSA employees must understand and adhere to all Executive Branch and OMIS Information Security and Privacy policies and procedures.

3.16 Use of External Information Systems Containing FTI

3.16.1 In accordance with IRS Publication 1075, DH, DHF, DoHS and OSA employees and contractors are prohibited from the following:

3.16.1.1 Accessing FTI from external information systems;

3.16.1.2 Using Department-controlled portable storage devices (e.g., USB drives, external hard drives) containing FTI on external information systems, unless approved by the IRS Office of Safeguards; and

3.16.1.3 Using non-department-owned information systems, system components, or devices to process, store, or transmit FTI. Any non-department-owned information system usage requires notification to the IRS Office of Safeguards 45 days prior to implementation.

3.16.2 Departments accessing and using FTI must enforce physical access at entry/exit points to facilities where the information systems that receive, process, store, or transmit FTI reside.

3.17 Change Management

3.17.1 Employees using removable media, USB devices, and related software for backup, transfer, temporary data storage, or any other action within the State network must establish and follow secure change management procedures for the emergency amendment of any data that occurs outside normal functions and procedures. Amendments and changes must be properly

documented, approved by WVOT, and meet all applicable statutory and regulatory requirements.

3.17.2 Any exceptions to functions or procedures should reference an existing procedure or outline specific steps for requesting and submitting an exception or change to the standard. In addition, the exception statement should reiterate the need to comply with the current standard while change requests are under consideration. For more information, see WVOT-PO1015, *Change & Configuration Management.*

3.18 Breach Notification and Incident Reporting

3.18.1 All system users, whether employees or contractors for the Departments, are expected to be aware of federal and state policies, procedures, and guidelines related to incident reporting and the use of sensitive and restricted PHI, PII, SSA data, and FTI. These must be followed to effectively safeguard sensitive and/or restricted information and to ensure the security and integrity of the information contained within the State network.

3.18.2 DH, DHF, DoHS and the OSA employees are responsible for the physical security of media devices in their care and must take all reasonable precautions to prevent theft, vandalism, and/or the loss/disclosure of sensitive data. Employees are required to report lost or stolen devices immediately to the WVOT online Incident Reporting system: https://apps.wv.gov/ot/ir/ and then contact OMIS at DHHRIncident@wv.gov using the subject line "Incident". For more information, see OMIS Procedure #OP-30, *Incident Reporting and Response.*

3.18.3 In the event of a breach or an incident, records must contain enough information to reconstruct the data. At a minimum, this includes the following information:

(a) The name of the recipient;
(b) Signature of the recipient;
(c) Date/time media was received;
(d) Media control number and contents;
(e) Movement or routing information; and
(f) If disposed of, the date, time, and method of destruction.

3.18.4 As specified by WV State Code and Executive Branch and State Privacy Office policies, all employees, contractors of the Departments, and users of State systems must report suspected or detected information security breaches or unauthorized disclosures immediately after discovery. (For more information, see OMIS procedure OP-30, *Incident Reporting and Response*.)

3.19 Each bureau and office will conduct semi-annual inventories of removable media containing PII to identify any missing media/data. This inventory will be documented, and the media owner will be notified of the loss.

3.20 Each bureau and office will conduct a semi-annual inventory of PII collected, used, stored, and retained following WVOT data classification guidelines. For more information see WVOT-PO1006, *Data Classification*.

4.0 ENFORCEMENT

Violation of any OMIS policy by State employees will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. The State may also be required by law to report certain illegal activities to the proper enforcement agencies.

Violation of any OMIS policy by external entities, including business associates, contractors, and/or consultants, may result in the termination of the relationship and/or

associated privileges. Violations may also result in civil and criminal penalties as determined by federal and state laws and regulations.

5.0 DEFINITIONS

5.1 Availability – A guarantee of reliable access to information by authorized people.

5.2 Change Management - The discipline that guides how we prepare, equip, and support individuals to successfully adopt change to drive organizational success and outcomes.

5.3 Confidentiality – A set of rules that limits access to information.

5.4 Data Loss Prevention (DLP) – A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

5.5 Digital media – Digital media includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as diskettes, magnetic tapes, external/removable hard drives, USB drives, compact disks, and digital video disks.

5.6 Data Custodian – This individual is responsible for the safe custody, transport, storage of data, and implementation of business rules. This person will control access to restricted and sensitive information and monitor that data while it is being stored or transported.

5.7 Data Owner – The individual who owns or is accountable for a data asset. The Data Owner can authorize or deny access to certain data and is responsible for its accuracy, integrity, and timeliness.

5.8 Data Steward – This individual is responsible for carrying out data usage and security policies as determined through enterprise data governance initiatives, acting as a liaison between the IT department and the business side of an organization. The data steward is responsible for collecting, collating, and evaluating issues and problems with data.

5.9 Degaussing - A process that erases information stored on digital media by eliminating a magnetic field.

5.10 Employees – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For Information Technology and Security policy, the term "employee" shall include the following: contractors, subcontractors, contractors' employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the State to be subject to this policy. This definition does not create any additional rights or duties.

5.11 Federal Tax Information (FTI) – According to the IRS Publication 1075, FTI is defined as any return or return information received from the IRS or secondary sources, such as SSA, Federal Office of Child Support Enforcement, or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from return or return information.

5.12 Federal Information Processing Standards (FIPS) - A set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

5.13 Integrity – The assurance that the information is trustworthy and accurate.

5.14 Media Marking – This term is used when referring to the application or use of human-readable security attributes. Marking differs from labeling, which is used

when referring to the application or the use of security attributes concerning internal data structures within the information system.

5.15 National Institute of Standards and Technology (NIST) - A physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness.

5.16 Non-digital Media – Media that includes printed documents and imagery (e.g., paper, microfilm) containing PII, PHI, FTI, or SSA data.

5.17 Office of Management Information Services (OMIS) - Office that reports directly to the DH, DHF, DoHS and the OSA Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Departments.

5.18 Personally Identifiable Information (PII) – All information that identifies, or can be used to identify, locate, or contact (or impersonate) a particular individual. Personally identifiable information is contained in both public and non-public records. Examples may include but are not limited to a specific individual's first name (or initial) and last name (current or former); geographical address, electronic address (including an e-mail address); telephone number or fax number dedicated to contacting the individual at their physical place of residence; social security number; credit and debit card numbers; financial records, including loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints; facial recognition and iris scans; driver identification number; full face image; birth date; birth or adoption certificate number; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an Internet cookie; criminal history, etc. When connected with one or more of the items of information specified above, PII includes any other information

concerning an individual, that if disclosed, identifies or can be used to identify a specific individual physically or electronically.

5.19 Protected Health Information (PHI) - Individually identifiable health information that is received, created, maintained, or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual and relates to:

(a) Past, present or future physical or mental health or condition of an individual;
(b) The provision of health care to an individual; and
(c) The past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

5.20 System Owner – A person or an organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. system owner could be a Program Manager, an Application Manager, an IT Director, or an Engineering Director.

5.21 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. Seq*... The WVOT is responsible for establishing technology policy, creating and supporting technology infrastructure (including the provision of training), evaluating equipment and services, and reviewing information technology contracts.

6.0 REFERENCES/RELATED MATERIAL

6.1 NIST Special Publication (SP) 800-53

6.2 Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

6.3 IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies.*

6.4 West Virginia Code §5A-6-4, *Procedures for Sanitization, Retirement and Disposition of Information Technology Equipment*

6.5 WVOT-PO1001 – *Information Security Policy*

6.6 WVOT-PO1002 – *Acceptable Use of State-Issued Portable/Mobile Devices*

6.7 WVOT-PO1006 – *Data Classification*

6.8 WVOT-PO1011 - *Digital Media Protection*

6.9 OMIS Policy 0512 – *Information Security Policy*

6.10 OMIS Procedure #OP-30, *Incident Reporting and Response*.

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	May 16, 2024	Issue Date
Version 1.0.1	November 15, 2024	Revise Departments' acronyms throughout; fix and add hyperlinks; fix format issues
Version 2.0	February 10, 2025	Annual Review and Update – reviewed links, format, and language throughout