State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Office of Management Information Services (OMIS)
OMIS Policy # 0512 – Information Security

Revised: January 26 2026

1.0 PURPOSE

This policy defines information security standards for the protection of WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) (Departments) confidential and/or sensitive data {i.e. protected health information (PHI), personally identifiable information (PII), social security administration (SSA) data, payment card industry (PCI) data, and federal tax information (FTI)}. All authorized users are required to maintain the confidentiality, integrity, availability, and regulatory compliance of this data as it is stored, processed, and/or transmitted within the agency.

2.0 SCOPE

This policy applies to all authorized system users, including DH, DHF, DoHS and the OSA employees, business associates, and vendors, with access to confidential and/or sensitive information and the systems that store, access, or process that information.

The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources and is not necessarily all-inclusive. The principles set forth in this policy are applicable to all information technology and assets, in all formats, utilized by the agency.

3.0 POLICY

3.1 Information resources will be used only for intended purposes as defined by DH, DHF, DoHS and the OSA bureaus/offices, will be consistent with applicable state and federal laws, and will satisfy all mandated federal compliance requirements.

3.2 All Agency employees must comply with the guidelines set forth in West Virginia Office of Technology (WVOT) policy WVOT-PO1001, *Information Security Policy*, as well as all other applicable federal, state, and DHHR requirements, policies, and guidelines.

3.3 All IT assets, including hardware, software, and data, are owned by the State, unless established by a formal contractual agreement(s). Distribution comes

directly from WVOT at the time of imaging. Updates and new installations occur during monthly maintenance.

3.4 Employees are required to comply with legal protection granted to programs and data by copyright and license. Users will not install any software, including open source software, on State systems. The WVOT or its equivalent must authorize and install all software.

3.5 Users will utilize, maintain, disclose, and dispose of all information resources, regardless of medium, according to law, regulation, and/or policy. Prior to transport to any offsite location, the WVOT must ensure that all information resources are cleansed onsite. (See SB 142 §64-2-3 – *Procedures for Sanitation, Retirement, and Disposition of Information Technology Equipment*.)

3.6 Employees must have no expectation of privacy while using State-provided information resources (e.g. cell phones, laptops, internet, etc.).

3.7 The State reserves the right to filter internet site availability and monitor and review employee use as required for legal, audit, or legitimate authorized State operational or management purposes.

3.8 IT policies and procedures will be reviewed and updated annually, or as needed, to ensure compliance with current state and federal laws, regulations, and policies. Employees must periodically review both WVOT and OMIS policies and procedures for updates.

3.9 Information Resources

3.9.1 Information resources are designated for authorized purposes only. The State has a right to review questionable employee activity. Only minimal personal use of State-provided IT resources is permitted (e.g. 10-15 minutes during break and/or lunch periods) and must not interfere with the legitimate business of the State.

3.9.2 Bureau Commissioners, Office Directors, and/or their organizational equivalent(s) are responsible for the protection of information resources under their jurisdiction and control.

3.9.3 All Agency employees are accountable for their actions relating to the integrity of the data within the information resources.

3.9.3.1 Agencies will work with WVOT to ensure that continuity of information resources supports critical governmental services in the event of a disaster
or business disruption.

3.9.3.2 Security requirements must be identified, documented, and addressed in all phases of development or procurement of information resources and satisfy all mandated federal compliance requirements.

3.10 All employees must adhere to rules regarding unacceptable uses of IT resources, as outlined in appendix "A" of WVOT policy WVOT-PO1001. This includes, but is not limited to the following:

3.10.1 Employees must not use IT resources to violate any local, state, or federal laws or statutes.

3.10.2 Employees must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (e.g. downloading MP3 files and/or broadcast audio or video files).

3.10.3 Employees must not intentionally introduce a virus into a State-provided computer or withhold information necessary for effective virus control procedures.

3.10.4 Employees must not send or share confidential information for unauthorized purposes.

3.10.5 Employees must not attach or use devices on the State network that are not owned by the State or authorized by the WVOT.

3.10.6 Employees must never execute programs or open email attachments that have not been requested or come from an unknown source. If in doubt and lacking assurance from the sender, employees should contact the WVOT Service Desk for assistance.

3.10.7 Employees must never attempt to disable, defeat, or circumvent any security firewalls, proxies, web filtering programs, or other security controls.

3.10.8 Employees must not access or attempt to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypass State security and access control systems.

3.11 Employees are prohibited from knowingly, willfully, and without authorization, directly or indirectly, tampering with, stealing, attempting to sell, altering, damaging, or destroying any State-provided equipment. This includes, but is not limited to desktop computers, laptops, iPads, keyboards, monitors, scanners, mice, printers, etc.

3.12 Security and Privacy Incidents

3.12.1 All system users, whether employees or contractors, are expected to be aware of federal and state policies and requirements related to the use of PHI, PII, PCI, SSA data, and FTI. These must be

followed in order to effectively safeguard confidential information and to ensure the security and integrity of the information contained within the State network.

3.12.2 All users who access state systems, networks, and facilities must immediately report all suspected or detected security/privacy violations, unauthorized disclosures, and/or attempted security/privacy breaches concurrently to both the WVOT and the OMIS. For more information, see the Office of Management Information Services (OMIS) Procedure #OP-30, *Incident/Breach Reporting and Response.*

3.12.3 The Departments must provide written notification to any taxpayer whose FTI was subject to unauthorized access or disclosure when a disciplinary or adverse action is proposed against a Department employee responsible. The written notification must include the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431.

3.12.4 The Departments must confirm to the Office of Safeguards when the required written notification to the taxpayer is completed and of any pending media releases, including sharing a draft of the release, prior to distribution.

3.13 Confidential PHI, PII, or other sensitive data, when emailed, must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet. DHHR employees are prohibited from sending email containing FTI through the State email system, either in the body of an email or as an attachment. (See OMIS policy 0510, *Email Guidelines and Requirements.*) Faxing services, which allows for the encryption of faxes, integrates network fax and email into a single solution. Options are available from WVOT upon request.

3.14 Sending and Receiving Confidential Data via Fax Machine

3.14.1 Agency employees should not send or receive PII, PHI, or PCI via fax machines unless it cannot be sent over other, more secure channels (i.e. delivery by hand or encrypted email, etc.).

3.14.2 When sending or receiving faxes containing PHI or PII, the following conditions must be met:

3.14.2.1 Faxes must be sent to an authorized recipient(s) only;

3.14.2.2 Fax machines must be physically located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions, or fax machines must be located in a secured area with limited access;

3.14.2.3 Accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and

3.14.2.4 A cover sheet must be used that explicitly provides guidance to the recipient. This will include a notification of the sensitivity of the data and the need for protection, and a notice to any unintended recipients to telephone the sender to report the disclosure and confirm destruction of the information.

3.14.3 If for some reason, the fax machine is not located in a secure location and monitored, the sender must contact the recipient prior to sending the fax to ensure his or her availability to receive the document, to confirm the number of pages, and to verify the correct fax number. Once the recipient has received the

fax, the recipient should contact the sender to confirm receipt.

3.14.4 **Agency employees must not send FTI over fax machines under any circumstances.** As an alternative, employees may use the OMIS secure file transfer protocol (SFTP) as a means of file transfer. The SFTP form can be found at the following link: https://intranet.wvdhhr.org/mis/ftpform.php.

3.14.5 If an employee inadvertently faxes PII, PHI, PCI or FTI he/she must follow the security incident protocol outlined in Section 10, *Reporting Improper Inspections or Disclosures*, in IRS Publication 1075, and the incident reporting process in OMIS OP#30, *Incident Reporting*.

3.15 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, employees must inform their supervisor or manager immediately.

3.16 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.

3.16.1 All passwords are confidential and **must not** be shared under any circumstances.

3.16.2 Employees are expected to use strong passwords, which must conform to established standards, and will be changed, at designated intervals set forth by WVOT.

3.17 All access to computing resources will be granted on a need-to-use basis. Individual users will be assigned unique user IDs.

3.18 Each employee must be accountable for securing his or her computer and for any actions that can be identified to have originated from it. In the event an employee fails to do so, a screensaver will automatically lock after ten (10) minutes of inactivity.

3.19 The WVOT is responsible for provisioning network user accounts by adding, modifying, and deleting user access. OMIS will authorize all access modifications for DH, DHF, DoHS and the OSA.

3.19.1 When an employee transfers or is terminated, the designated approval authority must go to the following link: https://otsm.wv.gov/HEAT/Modules/SelfService/#knowledgeBase and submit a form to modify or disable all access, unless otherwise approved in writing by appropriate management.

3.20 The authorized head of each agency must assure that all employees sign a confidentiality agreement upon hire and annually thereafter. This confirms that the employee has read, fully comprehends, and will abide by State policies and procedures regarding privacy and information security.

3.21 The agency head must assure that all employees receive an appropriate background check (where applicable) consistent with legislative rule and West Virginia Division of Personnel policy.

3.22 Security Awareness Training

3.22.1 All DH, DHF, DoHS and the OSA employees must complete mandatory online information security awareness training annually. New employees will be required to complete the training within the first week of employment as part of job orientation.

3.22.2 The agency head must ensure that all employees, and others who access computer systems, receive sufficient training in policies and procedures, privacy and security requirements, correct use of information resources, and other administrative controls.

3.22.3 Employees with assigned security roles and responsibilities will receive role-based security training prior to receiving access to the information system or performing duties requiring access to FTI; when required by information system changes; and at least annually thereafter.

3.22.4 The OMIS Office of Quality and Compliance will ensure that any user with access to FTI receives disclosure awareness training, which will include the ways in which FTI security requirements are communicated to end users. Training will be user specific to ensure that all personnel receive appropriate instruction.

3.23 OMIS will work with bureaus and offices to establish, maintain, and monitor an inventory, which contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII (includes PHI and FTI). This inventory will be reviewed and updated annually.

3.24 Use of External Information Systems

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

3.24.1.1 Accessing FTI from external information systems;

3.24.1.2 Using agency-controlled portable storage devices (e.g.,

flash drives, external hard drives) containing FTI on external information systems, unless approved by the IRS Office of Safeguards; or

3.24.1.3 Using non-agency-owned information systems; system components; or devices to process, store, or transmit FTI; any non-agency-owned information system usage requires notification to the Office of Safeguards 45 days prior to implementation.

3.25 All information assets must be accounted for and have an assigned owner. Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.

3.26 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information, according to a common classification scheme outlined in WVOT-PO1006 – *Data Classification*. The information classification will be submitted and included in the data inventory (see Section 3.24).

3.27 In order to minimize the risk to privacy, PII (includes PHI, PCI and FTI) must not be used for research, testing, training, or any reason other than its specified purpose. FTI cannot be masked or hidden.

3.28 If at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

3.29 The OMIS Office of Quality and Compliance will collaborate with WVOT to ensure that a risk management program is implemented and documented, and that a risk analysis is conducted periodically. This Office will also oversee and ensure that cost effective contingency response and recovery plans are maintained, providing for prompt and effective

restoration of critical business functions in the event of an incident or disruptive event.

3.30 Physical Security

3.30.1 Information resource facilities must be physically secured by measures appropriate to their critical importance.

3.30.2 Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following:

- Logging off computer;
- Locking computer;
- Keeping a clean desk where hard copy documents and devices containing sensitive information are not accessible; and
- Locking file cabinets and drawers.

3.30.3 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

3.30.4 Equipment must be secured and protected from physical and environmental damage.

3.30.5 Equipment used outside State premises will be given an equal or greater degree of security protection as that of on-site information resource equipment.

3.30.6 The Departments bureaus and offices must ensure that information systems that receive, process, store, or transmit FTI (e.g. servers, mobile devices, notebook computers, printers, copiers, scanners, fax machines) protect the confidentiality and

integrity of transmitted information to prevent unauthorized disclosure of FTI. These systems must be physically located in secure areas with restricted access. In circumstances when secure access cannot be maintained, such as home work sites, remote terminals, or other office work sites, the equipment as well as the data, must receive the highest level of protection practical, including full disk encryption.

3.30.7 All computers and mobile devices containing FTI residing in an alternate work site must employ encryption mechanisms to ensure that confidential data may not be accessed if the computer is lost or stolen.

3.30.8 All computers, electronic media, and removable media containing FTI, if approved by the IRS (see 3.24.1.2), must be locked-up and/or kept in a secured area under the immediate protection and control of an authorized individual. When not in use, the media must be promptly returned to a proper storage area/container.

4.0 ENFORCEMENT

Violation of this 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 this policy by external entities, including business associates, contractors, consultants, and/or interconnected entities may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations that extend beyond termination of employment, agreement, and contract.

5.0 DEFINITIONS

5.1 **Access** – The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

5.2 **Access Controls** – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

5.3 **Authentication** – The process of verifying the identity of a user.

5.4 **Confidential Data –** Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

5.5 **Contractor** – Anyone who has a contract with the State or one of its entities.

5.6 **Employee** – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of 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 WVOT to be subject to this policy. This definition does not create any additional rights or duties.

5.7 **External Information Systems** – Any technology used to receive, process, transmit, or store FTI that is not owned and managed by the Agency.

5.8 **Faxing services** – Allows users to fax a single document to an individual, or to broadcast fax documents from a PC to fax groups or distribution list(s).

5.9 **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

source, 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.

5.10 **Firewalls** - A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.

5.11 **Information Assets** – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

5.12 **Information Resources** - Networks, systems, applications, and data including but not limited to, ePHI received, created, maintained or transmitted by the DHHR.

5.13 **Information Security** – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

5.14 **Information Security Administrator (ISA)** – The person designated by the agency head to assure the agency's compliance with State information security policies and procedures. The ISA is the agency's internal and external point of contact for all information security matters.

5.15 **Information Security Incident –** An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

5.16 **Information Technology (IT) –** The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

5.17 **Owner of Information** – The person(s) ultimately responsible for an application and its data viability.

5.18 **Password –** A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

5.19 **Payment Card Industry Data Security Standard (PCI DSS)** – A proprietary information security standard for organizations that handle branded credit cards from the major card schemes.

5.20 **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 email 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.

5.21 **Privacy Officer** – The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.

5.22 **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:

• Past, present or future physical or mental health or condition of an individual; • The provision of health care to an individual; and

• 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.

5.23 **Remote Access** - the ability to gain access to the State's network from outside the network perimeter. Common methods of communication from the remote computer to the network include, but are not limited to, Virtual Private Networks (VPN), web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.

5.24 **Risk Analysis** – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

5.25 **Role-Based Access** - Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

5.26 **Threat –** Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.

5.27 **User –** A person authorized to access an information resource.

5.28 **User Id –** A unique "name" by which each user is identified to a computer system.

5.29 **West Virginia Division of Personnel** – The Division of the Department of Administration established by West Virginia Code § 29-6-1 *et seq.,* which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.

6.0 REFERENCES/RELATED MATERIAL

6.1 Health Insurance Portability and Accountability Privacy Rule, 45 CFR 160 and 164

6.2 IRS Publication 1075 – "Tax Information Security Guidelines for Federal, State and Local Agencies"

6.3 "Records Management and Preservation of Essential Records Act", W. Va. Code §§ 5A-8-21, 22

6.4 "Confidentiality and Disclosure of Tax Returns and Return Information", W. Va. Code § 11-10-5d

6.5 WVOT – PO1001 – *Information Security Policy*

6.6 WVOT-PO1006 – *Data Classification*

6.7 WVOT – PO1005 – *Email Use Standards*

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

6.9 WVOT – PO1014 – *Malicious Software/Anti-Virus*

6.10 West Virginia Executive Branch Procedure WVEB-P101.1 – *Response to Unauthorized Disclosures*

6.11 OMIS Procedure OP30 – *Incident/Breach Reporting and Response*

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	04/07/2003	Original Effective Date
Version 2.0	05/11/2015	Revised to update all sections
Version 2.1	07/07/2015	Revised to update FTI language
Version 2.2	12/15/2016	Revised to add information related to faxing PHI, PII, and FTI
Version 2.3	09/17/2018	Annual Review and Updates
Version 2.4	03/19/2020	Annual Review – revised sections 3.12.4, 3.14.4, and 3.14.5
Version 2.5	03/25/2021	Annual Review
Version 2.6	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Overall review of content - Revised language throughout
Version 2.7	02/07/2023	Annual Review; updated policy links
Version 2.8	02/14/2024	Annual Update - changed “DHHR” to “Departments of Health, Health Facilities, Human Services, and Office of Shared Administration”, updated links, overall review of content, revised language throughout
Version 2.9	07/08/2024	As the result of IRS security assessment, added language in

		Sections 3.12.3 and 3.12.4
Version 2.9.1	11/15/2024	Revised link in section 3.14.4
Version 2.10	02/10/2025	Annual review and update - reviewed language and links throughout
Version 2.11	01/26/2026	Annual Review and update; reviewed language; updated links