State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0527: Security & Privacy Training

Revised: January 26, 2026

1.0 PURPOSE

The purpose of this policy is to establish the regulatory training requirements for employees of the WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and the Office of Shared Administration (OSA) (Departments). This policy ensures that all personnel who access, manage, or support security and privacy functions related to computer systems, applications, and classified or regulated data receive the appropriate training. The intent is to promote compliance, safeguard information, and equip employees with the knowledge necessary to perform their duties responsibly and securely.

2.0 SCOPE

This policy applies to all DH, DHF, DoHS and OSA employees, including independent contractors, business associates, vendors, and third-party contractors regardless of classification, rank, or seniority.

3.0 POLICY

3.1 Security Awareness Training

3.1.1 All DH, DHF, DoHS, and OSA employees are required to complete annual online training in information security and privacy awareness. New employees will be required to complete the training within the first week of employment as part of the onboarding process.

3.1.2 Bureau and Office directors and managers must ensure that all employees who access sensitive or critical systems or information receive appropriate training on policies and procedures, privacy and security requirements, proper use of information resources, and other necessary administrative controls.

3.1.3 The OMIS Quality and Compliance Unit will ensure that all DH, DHF, DoHS, and OSA employees with access to State systems receive disclosure awareness training, which will include the ways in which federal tax information (FTI) security requirements are communicated to end users. Training will be user specific to ensure that all personnel receive appropriate instruction.

3.2 All bureaus and offices within the Departments will establish, maintain, and monitor an inventory, which contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII){includes protected health information (PHI) and FTI}. This inventory will be reviewed and updated annually.

3.3 Employees who have designated security roles or responsibilities must complete the appropriate role-based security training before they are granted access to any information system or begin duties involving access to FTI. Employees are required to complete this training at least once each year, and must receive additional training whenever system changes impact their responsibilities.

3.4 OMIS will work with the West Virginia Office of Technology (WVOT) to establish all level(s) of security clearance, security and privacy training, and expert training required for employees with security and privacy functions. Training may be assigned to specific roles for the following purposes:

- To acquire, audit, maintain, access, support, develop, design, analyze, or manage classified, regulated data elements.
- To manage computer systems, software applications, enterprise applications, and/or network hardware.
- To remain current with areas of expertise, separation of duties, elevated or administrative rights, and cyber security response.
- For the purposes of emergency preparedness and operations, disaster recovery, and cross training.

3.5 Security Clearance

3.5.1 Security clearance may be determined and assigned to each position at the time of recruitment.

3.5.1.1 Basic Security and Privacy Clearance – All users have a basic security clearance, which allows for admittance to the facility and allows network access in the performance of essential job duties.

3.5.1.2 Elevated Security and Privacy Clearance – This is assigned to all positions that require elevated administrative privileges as designated by the supervisor, based on the position's responsibilities and tasks.

3.5.1.3 Cyber and Operational Emergency Security Clearance - This clearance is assigned to all personnel whose positions are critical during cyber security incidents and operational emergencies.

3.6 Security and Privacy Training Modules

3.6.1 General security and privacy awareness training modules ("General") are mandatory for all employees, regardless of job classification, and provide the baseline security and privacy training required across the organization.This training will be provided by the Executive Branch, Department, and/or federally regulated entities on an annual basis and will include general security and privacy awareness, such as data confidentiality and social engineering. All certificates of completion will be kept on file for five years and made available for audit reporting and investigative purposes. This level of training must be completed within five (5) days of the first date of employment.

3.6.2 Elevated administrative privileges training modules (i.e., "Elevated") are required of all employees with access to federal tax information (FTI), protected health information (PHI), personally identifiable information (PII), social security administration (SSA) data, payment card industry (PCI) data, sensitive data, and extremely critical data and systems as determined by WVOT-PO1006, *Data Classification*. Elevated administrative privileges training includes the required general security and privacy awareness modules, plus additional instruction specific to the responsibilities and risks of having elevated access. It focuses on secure system administration, proper handling of sensitive data, and the extra safeguards expected of anyone using privileged accounts. This level of training

must be completed within five (5) days of the first date of employment and conducted annually thereafter.

3.6.3 Licensure and Certificate Maintenance training modules (i.e., "Cert") are required of all employees whose positions require ongoing licensure and certification for specialties and expertise in order to remain current and up-to-date in their field or discipline.

3.6.4 Performance Assessment training modules (i.e., "Performance") are required of all employees whose employment performance assessment depends on accumulating educational credit hours during a performance evaluation period. This is to be decided by each employee's immediate supervisor during the employment performance assessment period and will be recorded and kept on file in the employee's personnel file as an official record. This may include and be in combination with licensure and certificate maintenance training.

3.6.5 Cyber Security and Emergency Operations training modules (i.e., "Ops") are required of all critical users with mandatory positions during times of cyber security incidents and operational emergencies. This training will be conducted annually and in cooperation with the WVOT cyber security strategic plans and operational disaster preparedness efforts.

3.6.6 Changes to training module requirements and other security and privacy training will be determined prior to authorizing access to computer network systems and confidential or sensitive data. Clearances and classifications may be changed due to any of the following instances:

3.6.6.1 Changes in specific duties inherent to the job position (including emergency operations);

3.6.6.2 Access privileges required to accomplish job assignments are altered and as authorized by designated approval authority (including administrative access and emergency operations);

3.6.6.3 A change in licensure and certification requirements and maintenance;

3.6.6.4 A modification in Employment Performance Appraisal (EPA) requirements.

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, and/or consultants, 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.

State of West Virginia

Departments of Health, Health Facilities, and Human Services

Office of Shared Administration

Office of Management Information Services (OMIS)

Policy #0527: Security & Privacy Training

Revised: January 26, 2026

5.0 DEFINITIONS

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

5.2 **Designated Approval Authority** - Executive Branch agency appointed employee to authorize individuals' access and modify access for that agency and must complete a network logon request form.

5.3 **Employment Performance Appraisal** - clearly-defined performance goals and objectives and increased employee involvement.

5.4 **Federal Tax Information (FTI)** - FTI is 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.

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

5.6 **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.

5.7 **Protected Health Information (PHI)** - With regard to HIPAA covered entities, individually identifiable health information, including demographic information, whether

oral or recorded in any form or medium, that relates to the individual's health, health care services and supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual including but not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; or the past, present or future payment for the provision of health care to an individual; and includes identity information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected health information does not include the following:

- Records covered by the Family Educational Right and Privacy Act.
- Employment records held by the entity in its role as employer (though use and dissemination of these records may be subject to other federal and state laws such as the Family and Medical Leave Act and West Virginia Workers' Compensation).

5.8 **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.

5.9 **Sensitive Personal Information (SPI)** – Sensitive PII: Those elements of PII that must receive heightened protection due to legal or policy requirements. Examples of Sensitive PII include, but are not limited to the following:

- Social Security numbers or other government-issued identification numbers
- Financial account numbers, credit/debit card numbers
- Medical or health information
- Biometric data (fingerprints, facial scans, voiceprints)
- Precise geolocation data
- Login credentials, passwords, security questions
- Information about race, ethnicity, religion, or sexual orientation when tied to an identifiable person

6.0 REFERENCES/RELATED MATERIAL

6.1 WV Executive Branch Privacy Policy WVEB-P101, Accountability

6.2 WV Executive Branch Privacy Policy WVEB-P106, Security Safeguards

6.3 WV Office of Technology Policy, WVOT-PO1001, Information Security

6.4 WV Office of Technology Policy, WVOT-PO1006, Data Classification

6.5 WV Office of Technology Policy WVOT-PO1021, Account Management

6.6 WV Department of Health and Human Resources, Policy Memorandum 2124, *Employee Development*

6.7 OMIS, Policy 0512, Information Security

6.8 OMIS Procedure OP-30, Incident Reporting and Response

6.9 NIST SP 800-16, Information Technology Security Training Requirements, April 1998

6.10 NIST SP 800-50, Building and Information Technology Security Awareness and Training Program, October 2003

6.11 NIST SP 800-53, Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations, Updated 09/23/2020

6.12 IRS Publication 1075, Revised 11/2021

6.13 Acceptable Risk Controls for Affordable Care Act (ACA), Medicaid, and Partner Entities (ARC-AMPE), 03/10/2025

State of West Virginia

Departments of Health, Health Facilities, and Human Services

Office of Shared Administration

Office of Management Information Services (OMIS)

Policy #0527: Security & Privacy Training

Revised: January 26, 2026

8.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	10/24/2016	Approved by CIO
Version 1.1	06/01/2018	Annual Review and minor formatting revisions
Version 1.2	09/17/2018	Annual Review
Version 1.3	03/19/2020	Annual Review – Added sections 3.1-3.3; updated numbering
Version 1.4	03/25/2021	Annual Review

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0527: Security & Privacy Training

Revised: January 26, 2026

Version 1.5	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Annual review of content - Revised language throughout
Version 1.6	02/07/2023	Annual review; updated links
Version 1.7	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 1.8	02/10/2025	Annual Review and Update
Version 1.9	01/26/2026	Annual Review and update - revised language in section 3.0; revised definitions; fixed formatting issues