State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #538: Personnel Security

Revised: April 14, 2026

1.0 PURPOSE

All employees and third-party personnel, i.e., contractors, service providers, and vendors, within the WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) are responsible for systems and data security. To maintain security best practices, the Agencies will establish and adhere to an effective security planning program by following the required standards for managing risks from personnel screening, management, termination, and third-party access.

This policy defines the DH, DHF, DoHS and the OSA requirements for personnel security controls, outlines how and where they should be applied, and describes processes to mitigate the risk of unauthorized access to State data, electronic systems, and physical premises.

2.0 SCOPE

The security planning program is intended to safeguard employees, as well as information systems and assets, containing confidential 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}, which are used, managed, or operated by the Agency, contractors, or other organization(s) 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.

3.0 POLICY

3.1 Authority, Responsibility, and Duties

3.1.1 All DH, DHF, DoHS and OSA personnel are expected to execute appropriate security processes and/or activities to protect State information systems and assets, maintain proper safeguards, and ensure the unauthorized access, disclosure, modification, destruction, and/or interference of IT systems and data.

3.1.2 The Agencies' Security Program roles and responsibilities are assigned to specific personnel and may differ from the actual role or working title of the employee's position. Employees may be assigned multiple roles, only if the assignments provide sufficient separation of duties, adequate protection against the possibility of fraud, and do not lead to a conflict of interest. The Agency will utilize the following roles:

3.1.2.1 System Owner: This person or organization is responsible for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system. The system owner will ensure the availability, security, compliance, and support of the data residing on the system. The system owner will also work with the data owner to ensure that user access is reviewed at least annually, or as needed, to determine if access granted is still warranted.

3.1.2.2 System Administrator: This person is responsible for managing, troubleshooting, licensing, and updating hardware and software assets. He/she works closely with IT personnel and applicable employees to update systems, address security breaches, and help troubleshoot issues. The system administrator will plan for problematic situations and create procedures to restore computer systems and their functionality. Once notified that an individual has terminated employment or transferred to another state agency, or bureau/office within DH, DHF, DoHS and the OSA, the system administrator is responsible for the timely removal or adjustment of user access.

3.1.2.3 Management: IT Managers are responsible for operations, coordination, planning, and leading system-related activities within the Agency. They help determine the IT needs of the Agency and are responsible for both the implementation of information systems and the completion of requirements. When an employee transfers or is terminated, managers must ensure the DAA notifies the WV Office of Technology (WVOT) and other applicable system administrators, if appropriate, to modify or disable all access. It is also the manager's responsibility to notify appropriate system owners when vendor and contractor contracts expire, and access is no longer needed.

3.1.2.4 Human Resources: Human Resources will alert appropriate management, system owners, and key personnel in a timely manner when employees are terminated, resign, or transfer from their current position(s). For auditing purposes, Human Resources will provide a list of active employees upon request.

3.1.2.5 All Users of Electronic Resources and Systems: All users are accountable for any activity performed on the State network. Users must ensure that information resources will be used only for intended purposes as defined by Agency bureaus/offices, will be consistent with applicable state and federal laws, and will satisfy all mandated federal compliance requirements. All users must take necessary precautions to secure all State-owned equipment and proprietary information in their possession, and are responsible for returning all State-owned equipment upon termination or resignation.

3.1.3 The WVOT has established standards for creating, issuing, deleting, monitoring, and managing all Executive Branch employee network accounts. Name changes, accounting changes, and permission changes are

all documented. (See Office of Management Information Services (OMIS) Policy 0522, *Account Access*, for more information.)

3.1.4 The OMIS will work with agency bureaus and offices to review user accounts to ensure that access and account privileges are proportionate with job function, need-to-know, and employment status.

3.2 PS-1 – Personnel Security

3.2.1 All agency information assets must meet the required security controls defined in this policy, which are based on the National Institute of Standards and Technology (NIST) SP 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*.

3.2.2 All employees must adhere to this policy, which outlines the Personnel Security requirements the Agency will develop and/or follow, to protect the confidentiality, integrity, and availability of agency mission critical information.

3.2.3 This policy will be reviewed annually, at a minimum.

3.3 PS-2 – Position Risk Designation

3.3.1 In order to provide general guidance on the various security roles and responsibilities within the agency, the OMIS will assign information security job descriptions and responsibilities for the Agency's information security program.

3.3.2 The OMIS Information Security Officer (ISO) will work with subject matter experts within OMIS to assign a risk designation to all system user positions and establish screening criteria for individuals filling those positions. To clearly define security job responsibilities for system custodians and other

managers with focused security positions, the ISO will consider the following:

3.3.2.1 Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible. Documenting for each asset shall include the following:

- Management's assignment of system responsibility to a specific manager/custodian.
- Manager/custodian acceptance of responsibility for the system.
- Detailed description of manager/custodian responsibilities.

3.3.2.2 Clearly defining and documenting the agreed-upon authorization levels the position holder will have to ensure that he/she may effectively perform his/her job duties.

3.3.3 The OMIS will review, and revise position risk designations annually, or as needed, upon position vacancy or change in position description.

3.3.4 The OMIS will ensure that position risk designations are consistent with the requirements stated in the job classification policies published by the West Virginia Division of Personnel (DOP).

3.4 PS-3 – Personnel Screening

3.4.1 The OMIS will define IT personnel screening activities to reflect applicable federal and/or state laws, regulations, policies, standards, and specific criteria established for the risk designations of assigned positions. This includes, but may not be limited to the following:

3.4.1.1 Conducting background investigations, if applicable, prior to authorizing access to agency information and information systems.

3.4.1.2 Rescreening individuals, every five years, or as needed, and maintaining compliance with the State's personnel screening procedures.

3.4.1.2.1 West Virginia Senate Bill 88 requires the rescreening of individuals in a manner consistent with the criticality and sensitivity risk designation of their positions. Under this policy, the Criminal Identification Bureau (CIB) and the Federal Bureau of Investigation (FBI) shall retain applicant fingerprints to support ongoing determinations of an individual's suitability or fitness for a permit, license, or employment.

3.4.1.3 Ensuring screening procedures are consistent with the following:

- OMIS policy, regulations, and guidance.
- IRS Publication 1075 guidance for systems containing FTI.
- Federal guidance for systems containing PHI, PII, SSA data, and PCI data.
- The criteria established for the risk designation of the assigned position.

3.5 PS-4 - Personnel Termination

3.5.1 The WVOT has established standards for disabling all Executive Branch employee network accounts. All account changes are documented.

3.5.2 When an employee is terminated, his/her supervisor will complete and submit a Network Logon Request Form. All employee network deprovision

requests will be sent through the WVOT IT Support Portal, https://otsm.wv.gov/HEAT/Modules/SelfService/#serviceCatalog. All Request Forms must have documented approval. User accounts will not be disabled until the authorization process and required documentation is completed.

3.5.3 Each Agency will appoint one (or more) employees to serve as the designated approval authority (DAA). This employee(s) will authorize all access modifications for the Agency. When an employee is terminated, the DAA must do the following:

3.5.3.1 Contact WVOT as soon as possible to request all access be disabled within three (3) business days, unless otherwise approved in writing by appropriate management.

3.5.3.2 Complete and submit a Request Form following the "deleting a user id" procedure.

3.5.4 Upon termination of an individual's employment, WVOT will do the following:

3.5.4.1 Disable all information system access within three (3) business days upon notification of termination (See WVOT-PO1021, *Account Management*).

3.5.4.2 Disable user authenticators and credentials immediately upon the account owner's termination from work for the State or when the account owner no longer needs access to the system or application due to a leave of absence or temporary reassignment.

3.5.4.3 All accounts will be disabled but left intact for 30 days in case access or re-authorization is needed. After 30 days, the disabled account will be deleted.

3.5.5 The employee's supervisor will conduct an exit interview to ensure that terminated individual(s) understands the security constraints imposed by being a former employee, and that proper accountability is achieved for information system-related property.

3.5.6 Exit interviews will include, at a minimum, a discussion of confidentiality/non-disclosure agreements and potential limitations on future employment, as well as the review of Form OHRM-7C, the *WV DH, DHF, DoHS and OSA Departing and Transferring Employee Checklist.*

3.5.7 Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors.

3.5.8 During the exit interview, supervisors will be responsible for the following:

3.5.7.1 Recovering all information system-related property (e.g., keys, identification badges, State issued mobile devices including laptops, tablets, mobile phones, and hardware authentication tokens, etc.).

3.5.7.2 Ensuring that appropriate personnel retain access to data stored on the departing employee's information system.

3.5.7.3 Notifying the WVOT Service Desk, other relevant Service Desks (i.e., FA and CS), the WVOT Security Team, Agency building security, and other applicable OMIS management within three (3) business days upon notification of the employee's termination, or when there is the need to disable information system accounts prior to the employee(s) being notified of termination.

3.6 PS-5 - Personnel Transfer

3.6.1 When an employee transfers, his/her supervisor will complete and submit a Network Logon Request Form following the "Modify Employee" procedure. Requests will be sent through the WVOT IT Support Portal, https://otsm.wv.gov/HEAT/Modules/SelfService/#serviceCatalog. WVOT will modify all access to accommodate new user roles and responsibilities according to instructions from the DAA.

3.6.2 System Owners will work with System Administrators to review access logs and ensure the accuracy of information system(s) and facility access authorizations. Logs will be reviewed monthly, or as employees are reassigned or have transferred to other positions within the Agency.

3.6.2.1 The employee's manager at the previous work location is responsible for the following:

a. Ensuring the employee's equipment is cleansed/refurbished/recycled by WVOT.
b. Returning the employee's identification badges, keys, etc., as required.
c. Completing the Employee Network Account Request form within five (5) business days upon notification of transfer.
d. Removing or modifying all system, account, and facility access authorizations, as required.
e. Reviewing and signing the *WV DH, DHF, DoHS and the OSA Departing and Transferring Employee Checklist.*
f. Notifying agency personnel, as required.

3.6.2.2 The employee's manager at the new work location is responsible for the following:

a. Issuing new equipment.

b. Issuing the employee's identification badge(s), keys, etc. as required.
c. Completing the Employee Network Account Request form, outlining the applicable changes.
d. Providing access to systems, accounts, facilities, etc.
e. Ensuring the employee reviews and signs all applicable policies, procedures, and confidentiality agreements.
f. Notifying agency personnel as required.

3.7 PS-6 – Access Agreements

3.7.1 OMIS will ensure that appropriate agreements are completed before allowing DH, DHF, DoHS and the OSA employees, contractors, and other external entities, to access Agency information and information systems. Data owners will review and update agreements at least annually, or as needed. Types of agreements include, but may not be limited to the following:

- Non-disclosure/Confidentiality agreements
- System access agreements
- Acceptable use/Data use agreements
- Conflict-of-interest agreements
- Rules of Behavior

3.7.2 OMIS will ensure that individuals requesting access to Agency information and information systems complete the following processes:

3.7.2.1 Sign appropriate access agreements prior to being granted access. Agreements must include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.

3.7.2.2 Re-sign access agreements to maintain access to agency information and information systems at least annually or when access agreements have been updated.

3.7.2.3 Take all mandatory online information security and privacy awareness training annually. New employees will be required to complete the training within the first week of employment as part of job orientation. (For more information, see OMIS Policy #0527, *Security and Privacy Training*.)

3.7.2.4 Review and sign all Executive Branch and OMIS policies and procedures.

3.7.2.5 Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

3.7.3 All employee badge authorizations are reviewed annually to verify the correct level of facility access for each employee. This review shall be conducted by the employee's manager and/or OSA Central Facilities Management (CFM). All records are archived for 5 years.

3.8 PS-7 – Third-Party Personnel Security

3.8.1 OMIS will establish, document, and disseminate personnel security requirements, including security roles and responsibilities for third-party entities, and monitor compliance. These entities may include vendors, contractors, suppliers, service bureaus, and other external entities and/or organizations providing information system development, information technology services, outsourced applications, and/or security management.

3.8.2 Third-party providers must comply with Executive Branch and OMIS information security policies and procedures. Third-parties will be fully

accountable to the State for any actions taken while completing their Agency assignments.

3.8.3 In accordance with W. Va. Code § 15-2D-3 (e), the Director of the WV Division of Protective Services (DPS) requires any newly hired third-party vendors, contractors, and sub-contractors whose employees are regularly employed on the grounds or in the buildings of the State Capitol complex (this includes all Agency facilities), or who have access to sensitive or critical information, to submit to a fingerprint-based state and federal background check prior to receiving access to use State data and/or systems (see OMIS Policy #0529, *Vendor/Contractor Employee Background Checks*).

3.8.3.1 All third-party contracting companies will be informed during the contract award process that acceptance of any employee(s) permitted to access PHI, PII, FTI, SSA data, and/or PCI data is contingent upon proof of a favorable background check.

3.8.3.2 Prior to conducting a background check, a signed, written consent will be obtained from each applicant. Refusal to authorize the background check; failure to disclose a criminal conviction; or failure to provide truthful, accurate, and complete information will render the applicant ineligible for employment with the DH, DHF, DoHS and the OSA.

3.8.4 Agency contract managers will be responsible for communicating and enforcing applicable state and federal laws, requirements, policies, and procedures.

3.8.5 All third-party personnel must sign confidentiality agreement(s) prior to accessing State systems and/or data.

3.8.6 Agency operational and/or restricted information must not be released to third parties without properly executed contracts and confidentiality agreements. These contracts must specify conditions of use and security requirements and the access, roles and responsibilities of the third-party before access is granted.

3.8.7 Access must be granted to third-party users only when required for performing work, and with the full knowledge and prior approval of the information asset owner. The State utilizes the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks.

3.8.8 All new connections between third parties and the Agency must be documented in an agreement that includes information technology security requirements for the connections. Agreements will be signed by the applicable Agency Cabinet Secretary or his/her designee, and by a representative who is legally authorized to sign on behalf of the third-party. Both parties will keep the signed document on file.

3.8.9 Third parties must notify the OMIS Chief Information Officer (CIO), or his/her designee, of any transfers or terminations of contracted staff who possess organizational credentials or badges, or who have information system privileges as soon as transfers or terminations are known. A justification for the replacement request will be submitted to the CIO for review and approval.

3.8.10 OMIS will report third-party transfers or terminations to WVOT and Agency system owners, if applicable, by security-related characteristics. This may include the individual's functions, roles, and associated credentials/privileges, etc.

3.8.11 Third-party personnel providing offsite hosting or cloud services will be required to provide an annual independent risk assessment report, as well as a System Security Plan (SSP), if applicable, to the State to establish and maintain compliance with federal requirements. This may include, but is not limited to the Center for Medicare and Medicaid Services (CMS), the Social Security Administration (SSA), the federal Office of Child Support Enforcement (OCSE), the Internal Revenue Service (IRS), etc.

3.8.12 DH, DHF, DoHS and the OSA bureaus and offices are responsible for monitoring third-party provider compliance.

3.9 PS-8 – Personnel Sanctions

3.9.1 The DH, DHF, DoHS and the OSA utilize a formal sanctions process for Agency personnel failing to comply with established information security and privacy policies and procedures.

3.9.2 Agency bureaus and/offices will notify the OSA Office of Human Resources Management (OHRM) within 24 hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction(s).

3.9.3 OHRM will work with Agencies to ensure the sanctions process is consistent with applicable federal laws, directives, regulations, policies, standards, and guidance. Sanctions processes may be outlined in confidentiality and access agreements, employee disciplinary policies, and procedures published by the OHRM.

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, third-party contractors or personnel, 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 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.

5.2 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.

5.3 National Institute of Standards and Technology (NIST) – A non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote

U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

5.4 Office of Management Information Services (OMIS) - This office reports directly to the DH, DHF, DoHS and the 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.

5.5 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.

5.6 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.

5.7 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
- Credit card numbers
- Health and medical data
- Driver license numbers
- Individual financial account numbers

5.8 Social Security Administration (SSA) Data – Data received and accessed from the SSA for purposes of administering federally funded and state administered programs [i.e., Medicaid, Supplemental Nutrition Assistance Program (SNAP), and State Health Insurance Programs], which determines individual eligibility, citizenship status, and social security number verifications, etc.

5.9 System Security Plan (SSP) – A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

5.10 Third-party personnel – The service personnel, including subcontractors, of any third party engaged by an organization to provide services. Third-party personnel includes, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. Organizations explicitly include personnel security requirements in acquisition-related

documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by the organization.

5.11 West Virginia Division of Personnel (DOP) – The WV Division of Personnel supports WV state agencies in employing and retaining individuals of the highest ability and integrity by providing efficient and effective governmental services for the citizens of West Virginia, creating an environment that engenders trust and confidence at all levels, and creating an environment that promotes personal and professional growth.

5.12 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a, *et. seq.,* which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services and reviewing information technology contracts.

6.0 REFERENCES/RELATED MATERIAL

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

6.2 National Institute of Standards and Technology (NIST) SP 800-53, Security and Privacy Controls

6.3 WV Senate Bill 88

6.4 West Virginia Division of Personnel (DOP) website

6.5 WVOT - PO1021 – *Account Management policy*

6.6 WVOT – PO1001 – *Information Security policy*

6.7 OMIS Policy 0522 – *Account Access policy*

6.8 OMIS Policy 0512 – *Information Security policy*

6.9 OMIS Policy 0527 – *Security and Privacy Training policy*

6.10 OMIS Policy 0529 – *OMIS Vendor/Contractor Background Checks*

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	11/29/2021	Approved by DHHR CIO
Version 1.1	02/07/2023	Annual Review; updated policy links; added language in Section 3.8 about fingerprint-based background checks for third-party contractors
Version 1.2	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 1.3	06/28/2024	As the result of IRS security assessment, revised and/or added language in Sections 3.5, 3.6, 3.9
Version 1.3.1	11/15/2024	Revised Departments' acronyms; updated and fixed links; fixed formatting
Version 1.4	02/10/2025	Annual Review and Update – reviewed links; reviewed language and formatting; removed Employee Acknowledgement Page

Revised: April 14, 2026

Version 1.5	01/23/2026	Annual Review - Reviewed language and links; added link for WV SB 88
Version 1.5.1	04/14/2026	Revised section 3.9.2 notification timeframe from 72 hours to 24 hours per CMS requirements