State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0523 – Audit Controls

Revised: February 10, 2025

1.0 PURPOSE

Periodic security audits, both internal and external, are performed for the benefit of the WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) and its employees to: (1) identify weaknesses, deficiencies, and areas of vulnerability in operations; (2) assess compliance with federal, state, and agency laws, policies, procedures, and guidelines; (3) identify equipment and other physical safeguards and control systems that are inoperable, inappropriate, or inadequate; (4) review the effective application of security resources; and (5) identify and share "best practices" throughout the agency.

Just as auditing gives credibility to the information provided to auditors by an agency, audit controls provide applicable restrictions and act as a guide to good security practices within DH, DHF, DoHS, and the OSA and its bureaus and offices. By using automated audit controls, as available, all users, networks, and systems, as well as intranet and internet activities, can be recorded and tracked in order to safeguard assets, maintain data integrity, and ensure all systems are operating effectively.

This policy provides the framework for information system and physical security audits, identifies the roles and responsibilities of employees during internal and external audits, and defines audit controls and report structure within DH, DHF, DoHS, and the OSA. It also outlines audit control mechanisms and review processes utilized to enforce the use of personally identifiable information (PII) internally as identified in the Privacy Act and/or in public notices and contracted agreements.

2.0 SCOPE

This policy applies to all authorized systems and users, which includes, but is not limited to DH, DHF, DoHS, and the OSA employees, county offices, local health departments, business associates, contractors, and/or consultants, as they view and/or access resources granted and provided by the Departments.

Revised: February 10, 2025

3.0 POLICY

3.1 Security audits will be performed to ensure that information resources within DH, DHF, DoHS, and the OSA containing federally regulated and protected data are identified, monitored, and reviewed. This includes federal tax information (FTI), Social Security Administration data (SSA), protected health information (PHI), electronic protected health information (e-PHI), payment card industry data (PCI), and/or other proprietary and confidential information, as defined by West Virginia Office of Technology (WVOT) Policy WVOT-PO1006, *Data Classification*.

3.2 IT systems containing sensitive data will be assessed at least once every three (3) years.

3.3 State-owned/hosted information system(s) and those hosted by vendors, and/or the WVOT, must perform the following audit functions:

3.3.1 Automatically generate audit records and reports containing details (e.g., accounts, users, transactions, actions, date, time, location, subject, data type, systems) related to authorized and unauthorized activity, or malfunctions that occur. Event reporting capabilities must be enabled for system(s), account(s), and user(s) activity.

3.3.2 Store each entry in the audit file as a separate record.

3.3.3 Create transaction files to capture all input from interactive internet and intranet network applications.

3.3.4 Monitor system operational status using operating systems or audit logs to verify system functions and performance. Logs must be capable of

reproducing details of unauthorized activity, malfunction, or audit events identified by type, location, or subject;

3.3.5 Provide warnings and alerts to designated WVOT and Office of Management Information Services (OMIS) officials in the event of an audit processing failure.

3.3.6 Provide warnings and alerts to designated WVOT and OMIS officials when allocated audit record storage volumes reach 80 percent of the repository's maximum audit record storage capacity.

3.3.7 Protect audit information and audit tools from unauthorized access, modification, and deletion;

3.3.8 Allow designated agency officials to select which events are to be audited by specific components of the information system; and

3.3.9 Provide audit record generation capability and generate the audit records, for the auditable events as outlined in Control AU-2: Audit Events within the MARS-E System Security Plan (SSP) and Section 9.3.3.2, Audit Events, of IRS Publication 1075.

3.4 The agency must authorize access to manage audit functionality only to designated security administrator(s). System and network administrators must not have the ability to modify or delete audit log entries.

3.4.1 Results of these audits are confidential. OMIS must retain inspection reports, including a record of corrective actions, for three (3) years from the date the inspection was completed.

3.4.2 OMIS must retain audit records online for at least ninety (90) days and archive old records for ten (10) years to provide support for post investigations of security incidents, and to meet federal and state

regulatory requirements, as well as Executive Branch and the DH, DHF, DoHS, and OSA information retention requirements.

3.5 Audit logs must capture and preserve information needed to assist in preventing, detecting, containing, and mitigating information security violations. Logging should occur automatically, as available, within all State information systems and programs. Audit records will be generated when subjects (e.g. system users or automated processes) perform business related activities with system resources (e.g. files, database objects), and/or when adversaries attempt to perform unauthorized activities on the system resources. Each audit record will capture the details related to the underlying event and must include the following:

- Date and time of the event;
- Component of the information system (e.g., software or hardware component) where the event occurred;
- Type of event;
- Unique ID of the user;
- Outcome (success or failure) of the event;
- Execution of privileged functions; and
- Command line (for process creation events).

3.6 Controls must be adopted and maintained to help protect the audit log from unauthorized access or environmental damage. Audit log procedures must provide the following:

- Access controls to both printed and electronic audit logs.
- Separation of duties between personnel who control access and those who review the audit logs of access, whenever possible. This will include the following:
  a. Separating the duties of individuals, as necessary, to prevent malicious activity;
  b. Documenting separation of duties;

c. Defining information system access authorizations to support separation of duties;
d. Ensuring that audit functions are not performed by security personnel who are responsible for administering access control;
e. Auditing and maintaining a limited group of administrators with access based upon the users' roles and responsibilities and privileged and administrative accounts;
f. Ensuring that critical mission functions and information system support functions are divided among separate individuals;
g. Ensuring that information system testing functions (i.e., user acceptance,
quality assurance, and information security) and production functions are divided among separate individuals or groups; and
h. Ensuring that an independent entity - not the Business Owner, System Developer(s)/Maintainer(s), or Administrator(s) responsible for the information system - conducts security testing of the information system.

- Protection for audit data against overwriting, destruction or change;
- Documentation of regular use, review, and backup of the audit logs and any other records of information system activity which might help to prevent, detect, contain, and mitigate information security violations.

3.7 WVOT and OMIS will work together to ensure that the confidentiality, integrity, and availability of audit logs and audit log backups are protected from the date of creation and at least until the log retention expires, in accordance with Executive Branch, state, and federal retention requirements.

3.8 Controls for Information System Security Audits

3.8.1 Baseline documentation will be kept current and modified according to WVOT-PO1015, *Change and Configuration Management* policy, and will include the following:

3.8.1.1 An audit log profile/baseline representing normal system activity.

3.8.1.2 Guidelines/procedures for spotting and mitigating unusual system activity.

3.8.1.3 Audit control and review processes developed by each DH, DHF, DoHS, and the OSA bureau/office. This will include the following:

- The procedures to capture, retrieve, and review all audit logs and activity reports.
- Identification of the positions within the agency with the responsibilities and authority to review audit logs with assigned elevated administrative privileges based on "need to know," "least privilege," and "separation of duties."
- Details of how the system owner will periodically confirm that the logs within their bureau or office are reviewed.

3.9 The information system will provide an audit reduction and report generation capability that:

3.9.1 Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents;

3.9.2 Does not alter the original content or time marking of audit records; and

3.9.3 Allows for collected audit information and organizes such information in a summary format that is more meaningful to analyze.

3.10 The information system will compile audit records from defined information system components into a system-wide (logical or physical), time-correlated audit trail.

3.11 The DH, DHF, DoHS, and the OSA will work with OMIS and WVOT, as well as applicable vendors and contractors to employ automated mechanisms, as available, to integrate audit review, analysis, and reporting practices to support organizational processes for investigation and response to suspicious activities.

3.12 Physical Security Audits

3.12.1 The DH, DHF, DoHS, and the OSA bureaus and offices will ensure that sufficient procedures relating to physical access to buildings are developed and maintained. Access procedures will vary according to the individual office location.

3.1.2.1.1 State employees must always wear their State-issued ID badges in a conspicuous location above the waist while working in State facilities. Employees who cannot prominently display ID badge(s) due to safety reasons shall keep the ID badge(s) on his/her person and must produce it, upon request, to confirm identity. Employees who refuse or fail to display or produce their ID badge(s) shall be barred from entering State facilities and may be subject to disciplinary action.

3.1.2.1.2 Employees must use State-issued proximity cards when entering facilities that require the use of a proximity card. Employees who lose or misplace their cards must go through the same screening process as visitors and other non-employees. Employees who refuse to submit to this screening, or loan or permit another person to use their proximity card will be subject to disciplinary action.

3.12.2 Each bureau and office is responsible for conducting annual testing and review of its physical security plans. This includes environmental and equipment testing. Bureaus and offices may collaborate with WVOT,

OMIS, and/or the Office of Central Facilities Management, when necessary.

3.12.3 Each Department's bureaus and offices will issue authorization credentials for facility access. These lists must be reviewed at least annually. Employees will be immediately removed from facility access when access is no longer necessary, unless otherwise approved in writing by appropriate management.

3.12.4 The DH, DHF, DoHS, and the OSA will work with OMIS, WVOT and applicable contractors to enforce physical access authorizations to the information system, as well as the physical access controls for the facility, in locations where federal tax information (FTI) is received, processed, stored, or transmitted.

3.12.5 All information resource facilities must be physically protected in proportion to the criticality or importance of their function(s). Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently, depending on the nature of the systems being protected.

3.12.6 Access to facilities housing critical state IT infrastructure, systems, and programs must follow the principle of least privilege access. Personnel, including full and part-time staff, contractors, and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.

3.12.7 The process for granting physical access to State information resource facilities must include the approval of the OMIS Chief Information Officer (CIO), or his or her designee. Access reviews must be conducted at least quarterly, or more frequently, depending upon the nature of the systems being protected. Removal of individuals who no longer require access must be completed in a timely manner.

3.12.8 Visitor access logs must be reviewed at least monthly by two (2) separate approval authorities and maintained for five (5) years. When visiting information resource facilities housing State data, all individuals must:

- Check-in with security or authorized personnel;
- Sign-in and out on a visitor's log;
- Provide a reason for access;
- Show a valid picture ID;
- Wear a visitor's badge in a conspicuous location above the waist; and
- Be escorted at all times by an employee when in a secure area.

3.12.9 Bureaus and Offices within the DH, DHF, DoHS, and the OSA undergoing physical security audits, whether internal or external, must adhere to the following guidelines:

3.12.9.1 Bureaus and/or offices located either at the Diamond Building or One Davis Square in Charleston, must contact the Central Facilities Management Office at least 14 days prior to the audit to ensure appropriate collaboration and response.

3.12.9.2 Community Services Managers (CSM) and Regional Directors (RD) at Department of Human Services' county offices are responsible for coordinating with auditors concerning all aspects of physical security at their respective location(s).

3.12.9.3 Security personnel and/or hospital administrators at county hospitals are responsible for coordinating with auditors concerning all aspects of physical security at their respective location(s).

3.12.9.4 A list of contacts will be maintained by each entity and reviewed and updated on an annual basis.

3.13 IRS Audit Guidelines for FTI

3.13.1 Security-relevant events must enable the detection of unauthorized access to FTI data. Auditing must be enabled to the greatest extent necessary to capture access, modification, deletion, and movement of FTI by each unique user.

3.13.2 Access control systems (e.g., badge readers, smart cards, biometrics, etc.) providing the capability to audit access control attempts must maintain audit records with successful and failed access attempts to secure areas containing FTI or systems that process FTI. Access control logs must be reviewed on a monthly basis. The logs must contain the following elements:

- Owner of the access control device requesting access
- Success/failure of the request
- Date and time of the request

3.13.3 OMIS will collaborate with the DoHS to perform internal reviews to ensure that the security policies and procedures established to protect FTI are applicable, maintained, and properly enforced. To provide adequate objectivity and separation of duties, these reviews should not be performed by the same group or entity that created the IT security policies, procedures, and controls being audited, or that manage the IT operations. Copies of these inspections must be submitted to the IRS with the Safeguard Security Report (SSR).

3.13.4 The DH, DHF, DoHS, and the OSA will establish the following review cycle(s):

- County offices receiving FTI: at least every three years;
- The contractor owned/managed consolidated data center: at least every 18 months;
- All contractors with access to FTI, including off-site storage facility: at least every 18 months.

3.13.5 The DoHS and OMIS will complete a documented schedule detailing the timing of all internal inspections in the current year and subsequent two (2) years (i.e., a three-year cycle). The plan must be included as part of the SSR.

3.13.6 The DoHS will retain all security inspection reports, including a record of corrective actions, for a minimum of five (5) years from the date the inspection was completed. A summary of the agency's findings and the actions taken to correct any deficiencies must be included with the SSR submitted to the IRS.

3.13.7 In order to track the movement of FTI, bureaus and offices are required by IRC 6103(p)(4)(A) to maintain a record of all internal and external requests made by or to them for disclosure of FTI. Records must be maintained for five (5) years, or the agency's records retention schedule must be followed, whichever is longer.

3.13.7.1 The DH, DHF, DoHS, and the OSA will establish, maintain, and monitor an inventory containing a list of all programs and information systems that collect, use, maintain, or share PII (includes PHI and FTI). This inventory will be reviewed and updated annually.

3.13.7.2 This inventory must be provided to the OMIS Information Security Officer (ISO) annually, or upon request, to support the establishment of information security requirements for all new or modified information systems containing FTI.

3.13.7.3 Records must be maintained in accordance with IRS audit log retention requirements for electronic and non-electronic files.

3.13.7.4 The agency must establish a tracking system to identify and track the location of electronic and non-electronic FTI from receipt until it is destroyed. The FTI log may include tracking elements, such as:

- Taxpayer Name or other identifier
- Tax year(s)
- Type of information (e.g., revenue agent reports, Form 1040, work papers)
- The reason for the request
- Date requested
- Date received
- Exact location of the FTI
- Who has had access to the data
- If disposed of, the date and method of disposition
- To the extent possible, FTI must not be included in the log. If FTI is used, the log must be secured in accordance with all other safeguards requirements (see Pub 1075 for more information).

3.13.7.5 Disclosures outside the agency to vendors or contractors must be recorded on a separate list or log. The log must reflect to whom the disclosure was made, what was disclosed and why, and when it was disclosed.

3.13.7.6 Employees are prohibited from disclosing FTI to either internal or external auditors.

3.13.8 Secure storage - Each bureau and office must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive or confidential data on digital and non-digital media.

3.13.9 Care must be taken to deny unauthorized access to areas containing FTI during work and non-work hours. This can be accomplished by creating restricted areas, security rooms, or locked rooms. Additionally, FTI in any form (computer printout, photocopies, tapes, notes) must be protected during non-work hours. This can be done through a combination of methods, including secured or locked perimeter, secured area, or containerization.

3.13.10 Unlimited access to areas containing FTI will only be granted to individuals whose daily work functions necessitate admittance. This includes employees who access FTI as part of their job and/or support staff whose responsibilities require that they perform system functions on servers or equipment.

3.13.11 To ensure that only authorized personnel have access to the areas that contain FTI, OMIS will identify which application programs use FTI and how access to that FTI is controlled.

3.13.12 All employees must protect electronic and physical media containing confidential and/or sensitive data while at rest, stored, or actively being accessed. (see OMIS policy #0524 - *Workstation Security*).

3.13.13 All Departments must ensure the proper storage of data and information files for which they are responsible. Secure storage includes locked drawers, desks, or cabinets, and/or a controlled media library; as well as locking or logging off the computer when not in the immediate vicinity of the work area. Employees must adhere to the following guidelines:

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

(b) Employees must protect the State's information and comply with the agency records retention policy (see policy – Records Retention and Disposal: http://intranet.wvdhhr.org/policies/Policies/Records%20Retention%20Schedule%209-30-16.pdf).

(c) 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 the State's information security standard for encryption.

(d) 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).

(e) Bureaus and offices 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*).

(f) Sensitive and/or confidential data stored on secondary storage devices (i.e. backups) must be encrypted, as required for the protection of the highest level of information contained therein.

(g) Bureaus and offices must maintain stored public data to a minimum of what is necessary to adequately perform business functions. If

sensitive and/or confidential 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. Bureaus and offices should remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the Departments' Records Retention and Disposal policy. This control is optional for LOW risk information systems.

3.13.14 Bureaus and offices receiving, processing, storing, or transmitting sensitive and/or confidential data 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.
   f. Changing combinations and keys at least annually, or when an employee retires, terminates employment, or transfers to another position.

3.13.15 Entry to Restricted Areas

3.13.15.1 Doors to Restricted Areas and Data Centers must always remain locked. Any main entrance must be controlled by a

staffed security desk to ensure that only authorized personnel with an official need may enter.

3.13.15.2 Restricted areas will be prominently posted and separated from non-restricted areas by physical barriers that control access. Entrances will have controlled access (e.g., electronic access control, key access, door monitor) to prevent unauthorized entry.

3.13.15.3 Every card reader door access is automatically logged 24/7 and all activity is retained for one year.

3.13.15.4 Only individuals authorized by management may have system administrator rights to the restricted area.

3.13.15.5 Unlimited access to restricted areas will only be granted to individuals whose daily work functions necessitate admittance.

3.13.15.6 A restricted area visitor log must be maintained at a designated entrance to the restricted area, and all visitors entering the area will be directed to the designated entrance.

3.13.15.7 Visitors must be always accompanied by authorized personnel. If the visitor has a clear need to enter an unauthorized area, the employee accompanying the visitor must use his/her badge to gain access both in and out.

3.13.15.8 All visitors must sign-in to the visitor access log, detailing the following information:

- Name and organization of the visitor
- Signature of the visitor

- Form of identification
- Date of access
- Time of entry and departure
- Purpose of visit
- Name and organization of person visited

3.13.15.9 Front desk personnel must validate a visitor's identity by examining government issued identification (e.g., WV state government ID, state driver's license) and recording in the access log the type of identification validated. The security personnel must compare the name and signature entered in the access log with the name and signature of the government-issued identification. When leaving the area, the security personnel or escort must enter the visitor's time of departure. If there is any doubt of the identity of the individual, the security monitor must verify the identity of the vendor/contractor individual against the access log prior to allowing entry into the restricted area.

3.13.15.10 Each restricted area access log must be closed out at the end of each month and reviewed by management.

3.13.15.11 To facilitate the entry of employees who have a frequent and continuing need to enter a restricted area, but who are not assigned to the area, an Authorization Form must be on file for each person who is authorized to enter. This file will be maintained by the OSA Director of Operations for a designated time period.

3.13.15.12 All individuals requesting access to the contractor owned and managed Data Center must have proper written authorization and justification from their director. Requests must be sent via email to WVOT.

3.13.15.13 The OSA Director of Operations, or a designee, will maintain an authorized list of all personnel who have access to information system areas, where these systems contain FTI. A list of authorized employees, contractors, and vendors will be reviewed and verified monthly.

3.13.15.14 Individuals are prohibited from "piggybacking" or "tailgating" into restricted locations. All individuals entering areas containing FTI must not bypass access controls or allow unauthorized entry of other individuals. Unauthorized access must be challenged by authorized individuals (e.g., those with access to FTI).

3.13.15.15 The Data Center contractor will monitor physical access to the facility to detect and respond to physical security incidents. For all areas that process FTI, Data Center staff will position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

3.13.15.16 OMIS will implement physical and technical safeguards for all workstations accessing FTI to restrict access to authorized users. Employees must guard against access to data and take precautions to protect IT devices when away from the workstation.

3.13.16 WVOT and OMIS will incorporate effective security controls to ensure that FTI is protected at all points where it is received, processed, stored, or transmitted. All information systems used for receiving, processing, storing, or transmitting FTI must be hardened in accordance with the requirements in IRS Publication 1075. This includes the equipment,

facilities, and employees/contractors that collect, process, store, display, and disseminate information. This applies to computers, hardware, software, and communications, as well as policies and procedures for their use.

3.13.17 Upon completion of use, the Departments must ensure that all FTI is destroyed or returned to the IRS or the Social Security Administration (SSA) according to IRS Pub 1075 guidelines. Users of FTI are required by IRC 6103(p)(4)(F) to take certain actions after using FTI to protect its confidentiality.

3.13.17.1 Officials and employees within the Departments must either return the information (including any copies made) to the office from which it was originally obtained or destroy the FTI. The Department of Human Services will include in its annual report (e.g., SSR) a description of the procedures implemented.

3.13.17.2 When returning IRS information, the Department of Human Services and OMIS will use an established receipt process and ensure that the confidentiality is protected at all times during transport. FTI furnished to the user and any paper material generated, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by shredding. If a method other than shredding is used, that method must make the FTI unreadable or unusable. Electronic media containing FTI must be destroyed according to Sections 9.3.10.6 and 9.4.7, Media Sanitation.

3.13.18 OMIS will collaborate with WVOT and system contractors to perform the following actions:

3.13.18.1 Create and maintain a System Security Plan (SSP), as well as policies, procedures and processes for the establishment, use, and auditing of non-local maintenance and diagnostic connections within the Departments.

3.13.18.2 Review and analyze all records related to non-local maintenance and diagnostic connections and sessions.

3.13.18.3 Review and analyze information system audit records at least weekly or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized FTI access.

3.13.18.4 Report findings according to Executive Branch and OMIS incident response procedures. If the finding involves a potential unauthorized disclosure of FTI, the appropriate entity, (i.e., Departments and the IRS Office of Safeguards officials) must be contacted. For more information see WVOT PO1001, *Information Security Policy* and OMIS procedure OP-30, *Incident Response and Reporting*.

3.14 WVOT Audit Responsibilities

3.14.1 Agencies engaged in any IT audit activity by third parties (e.g., IRS, CMS, SSA) are responsible for contacting the WVOT CSO Audit Team as soon as notification of the audit has been received. The WVOT Information Security Audit Program will synchronize third-party information security audit activities with WVOT services and units.

3.14.2 WVOT will examine, evaluate, and report on information technology (IT) applications, related systems, operations, processes, and practices for both internal and external audits.

3.14.3 The WVOT must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries. This requirement also applies to outsourced data centers or cloud providers. For additional information, see Section 3.16 of WVOT-PO1008, *Information Security Audit Policy.*

3.15 DH, DHF, DoHS and OSA Audit Responsibilities

3.15.1 The OMIS Office of Quality and Compliance is responsible for managing the IT security audit program for DH, DHF, DoHS, and the OSA. This unit will collaborate with WVOT, federal, state agencies, and/or contractors to coordinate both internal and external audits for all Department-owned information systems.

3.15.2 Each bureau and office within the DH, DHF, DoHS, and the OSA must perform the following tasks:

3.15.2.1 Review and analyze information system audit records at least weekly, or more frequently at the discretion of the information system owner for indications of unusual activity related to potential unauthorized access.

3.15.2.2 Partner with OMIS to report any unusual findings according to federal (e.g., IRS, SSA), Executive Branch, and Department incident response policy and procedures.

3.15.2.3 Ensure information in the audit file is retrievable by an automated method and produce records upon request.

3.15.2.4 Develop an Audit Control and Review Plan in conjunction with OMIS. The plan will include the following:

- A list of the systems and applications to be logged.
- The information to be logged for each system or application.
- The login reports for each system or application.
- Details of how the system owner will periodically confirm that the logs within their bureau or office are reviewed.
- The procedures to review all audit logs and activity reports.

3.15.3 The DH, DHF, DoHS, and the OSA must develop organizational-wide standard categories for the retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions, as well as standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provides federal policy on record retention and will be followed when Department retention schedules do not exist or have not been defined.

3.15.4 OMIS will collaborate with WVOT and bureaus and offices to analyze and compare audit records across different repositories to gain organization-wide situational awareness.

3.15.5 The OMIS Information Security Officer (ISO) will collaborate with federal entities, WVOT, and Departments' bureaus and offices to conduct information security risk assessment(s).

3.15.6 OMIS will work with bureaus and offices if needed, to create IT security audit plans. This will ensure the agency schedules the necessary IT security audits of any sensitive systems identified in data and system classification during the risk management process.

3.15.7 Each bureau and office will develop, approve, and maintain a list of employees with authorized access to IT resources and restricted areas within State office facilities.

3.15.8 OMIS will develop, document, and disseminate an up-to-date audit and accountability procedure, addressing purpose, scope, roles, responsibilities, management commitment, compliance, and coordination among agency entities. This document will be reviewed and updated annually.

3.15.9 OMIS will assist bureaus and offices, if needed, to monitor and audit privacy controls and internal privacy policy, as required, to ensure effective implementation.

3.15.10 The DH, DHF, DoHS, and the OSA will comply with all WV State Privacy Office monitoring and auditing policies and procedures.

3.16 External Audit Notification

3.16.1 Upon notice of an audit by external auditors, regulatory agencies, reviewers, and/or contractors, bureaus and offices must take the following steps:

3.16.1.1 Contact the WVOT Office of Information Security and Controls (OISC) Audit Team as soon as notification of an audit has been received. This unit will coordinate audit activities with all WVOT services and units.

3.16.1.2 Notify the Office of Shared Administration's Office of Internal Control and Policy Development (OICPD) of the audit, by completing a Notification Form. Audits and Reviews Conducted at or on the DH, DHF, DoHS, and the OSA by external auditors and regulatory entities. This Form must only be submitted under the following circumstances:

- If an external entity (e.g. Governor's Office, federal agency, State oversight agency) requires a Department to procure the services of an independent contractor to perform an audit or review.

- If an external entity (e.g. Governor's Office, federal agency, State oversight agency) procures the services of an independent contractor to perform an audit or review.

3.16.4 The Notification Form must be completed within five (5) days of receiving notice of an audit. It must be submitted via email.

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.

5.0 DEFINITIONS

5.1 **Audit Logs** – A security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

5.2 **Audit Report** – A document prepared by the auditors appointed to examine the organization's IT systems. Included in these types of reports is an Executive

Summary; Background Information, which includes Audit Objectives, Scope, Testing Approach, and Statement of Auditing Standards; and Findings, Observations, and Recommendations, which includes IT Policies and Procedures, IT Risk Assessment, Disaster Recovery Plans and a Self-Assessment Review.

5.3 **Containerization** - A form of virtualization where applications run in isolated user spaces, called containers, while using the same shared operating system (OS). A container is essentially a fully packaged and portable computing environment:

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

5.5 **Data Owner** – An entity who can authorize or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

5.6 **Electronic Protected Health Information (e-PHI)** - Protected health information means individually identifiable health information that is: transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

5.7 **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, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the DH, DHF, DoHS, and the OSA to be subject to this policy. This definition does not create any additional rights or duties.

5.8 **External Audit** – This type of audit, also known as a third-party audit, is performed by an audit organization independent of the customer-supplier relationship and is free of any conflict of interest. Independence of the audit organization is a key component of a third-party audit. These audits may result in

certification, registration, recognition, license approval, a citation, a fine, or a penalty issued by the third-party organization or an interested party.

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 **Internal Audit** – This type of audit is performed within an organization to measure its strengths and weaknesses against its own procedures or methods and/or against external standards adopted by (voluntary) or imposed on (mandatory) the organization. It is conducted by auditors who are employed by the organization being audited, but who have no vested interest in the audit results of the area being audited. An IT internal audit can play a critical role in evaluating the organization's information security strategy by confirming the right processes are in place to manage programs and ensuring processes and controls are being executed appropriately.

5.11 **Least Privilege** – Giving a user account only those privileges which are essential to that user's work.

5.12 **Office of Management Information Services (OMIS)** - This office reports directly to the Departments' Cabinet Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the WV Departments of Health, Health Facilities, Human Services, and the Office of Shared Administration.

5.13 **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.

5.14 **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.

5.15 **System Administrator** - Person responsible for running and maintaining the networked computers, peripherals, and the network itself. He or she, among other functions, (1) installs hardware and software, (2) issues login names, (3) maintains security, (4) fixes bugs and crashes, and (5) monitors the network. In case of a single desktop computer, the user often acts as the sys admin.

6.0 REFERENCES/RELATED MATERIAL

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

6.2 HIPAA §164.312 Technical Safeguards

6.3 45 CFR §155.260(a) of the Privacy Act

6.4 45 CFR §155.280 as it pertains to Federally facilitated Exchanges

6.5 WVOT – PO1008 – Information Security Auditing policy

6.6 WVOT – PO1001 – Information Security Policy

6.7 WVOT – PO1002 – Acceptable Use of Portable and/or Wireless Devices

6.8 WVOT – PO1006 – Data Classification

6.9 WVOT – PO1015 – Change and Configuration Management

6.10 Department Policy Memorandum OPS-40-0-1 - Diamond Building/One Davis Square Access

7.0 REVISION HISTORY

Version	Date	Revisions
Version 1.0	07/27/2017	Document Approved by CIO
Version 2.0	09/17/2018	Annual Review - added links
Version 2.1	11/14/2018	Added language in Section 3.13.7
Version 2.2	12/06/2019	Added language in Section 3.12.8 re: ID badges
Version 2.3	03/19/2020	Annual Review
Version 2.4	03/25/2021	Annual Review - updated language throughout
Version 2.5	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Overall review of content - Added new language in Section 3.13 re: IRS Audit Guidelines and Entry to Restricted Areas; Revised language throughout

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0523 – Audit Controls

Revised: February 10, 2025

Version 2.6	02/07/2023	Overall review of content; updated policy links; revised language throughout
Version 2.7	01/08/2024	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 2.8	02/10/2025	Annual Review and Update; Reviewed language, links, and format