State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0524: Workstation Security

Revised: February 10, 2025

1.0 PURPOSE

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}, as well as the technology and equipment used to maintain it, is a vital government asset; therefore, it must be protected at all times.

The purpose of this policy is to outline standards for securing electronic data and to reduce the risk to WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) equipment from internal and external threats. This policy defines expected employee behavior regarding the secure use of technology resources and the requirements for safeguarding State-provided equipment and workstations.

2.0 SCOPE

The scope of this policy includes the use of desktop workstations, laptops, and all client computing devices connected to the State network. It applies to all DH, DHF, DoHS and OSA employees and authorized system users, which includes, but is not limited to county offices, State hospitals, local health departments, business associates, contractors, and/or consultants as they fall within the authorization to access resources granted by the Departments.

3.0 POLICY

3.1 Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of confidential information, and that access to that information is restricted only to authorized users.

3.2 As outlined in OMIS Policy 0512, *Information Security*, each employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.

3.3 DH, DHF, DoHS and OSA employees must consider the sensitivity and confidentiality of the information, including PHI, PII, FTI, PCI, and SSA data that may be accessed, and minimize the possibility of unauthorized access.

3.4 OMIS will implement physical and technical safeguards for all workstations accessing confidential data 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. This includes, but may not be limited to the following:

- Logging off the computing device;
- Locking the computing device;
- Ensuring monitors are positioned away from public view, when possible; and
- Storing sensitive, private, and essential data on a local server (i.e. y: drive) rather than on the computing devices' internal hard-drives.

3.5 Password-protected screen savers will be enabled on all workstations/laptops with a time-out interval of ten (10) minutes. Users will be required to logon for re-entry.

3.6 When equipment is used outside of state premises, it and the data on it will be given an equal or greater degree of security protection as that of on-site information resource equipment and data.

3.7 Employees will not attempt to disable, defeat, or circumvent security controls.

4.0 ENFORCEMENT

Violation of any DH, DHF, DoHS and OSA policy by State employees will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including

termination. The State may also be required by law to report certain illegal activities to the proper enforcement agencies.

Violation of any DH, DHF, DoHS and OSA policy by external entities, including business associates, contractors, and/or consultants, may result in termination of the relationship and/or associated privileges. Violations may also result in civil and criminal penalties as determined by federal and state laws and regulations.

5.0 DEFINITIONS

5.1 **Availability** – a guarantee of reliable access to the information by authorized people.

5.2 **Confidentiality** – a set of rules that limits access to information.

5.3 **Employees** – 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.

5.4 **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.

5.5 **Integrity** – the assurance that the information is trustworthy and accurate.

5.6 **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.

5.7 **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.

5.8 **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 **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.

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

6.0 REFERENCES/RELATED MATERIAL

6.1 WVOT-PO1001 – *Information Security Policy*

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

6.3 OMIS Policy 0512 – *Information Security Policy*

6.4 OMIS Policy 0515 - *Acceptable Use of Wireless and Mobile Devices*

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	April 18, 2016	Approved by OMIS CIO

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0524: Workstation Security

Revised: February 10, 2025

Version 1.1	September 5, 2017	Annual Review and Revision. Two minor revisions: added section 3.3 and revised section 3.4
Version 1.2	September 18, 2018	Annual Review
Version 1.3	March 19, 2020	Annual Review
Version 1.4	March 25, 2021	Annual Review
Version 1.5	February 1, 2022	Converted document from Word to Google Docs; Updated formatting; Overall review of content - Revised language throughout
Version 1.6	02/07/2023	Annual Review; updated policy 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 2.0	02/10/2025	Annual Review - review content, links, and format