State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)

OMIS Policy #0515 – Acceptable Use of Wireless and Mobile Devices

Revised: February 10, 2025

1.0 PURPOSE

Wireless and mobile devices are made available to employees to assist them in the performance of their job duties. This policy defines standards, restrictions, and appropriate use for employees who have legitimate business reasons to access data from State-owned mobile devices and/or wireless communication service within the State network.

The WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and the Office of Shared Administration (OSA) and its employees must protect the integrity of the confidential data residing within the State's technology infrastructure; ensure the security of State-owned devices by preventing loss, damage, misuse, or theft; and certify that all State-owned devices are accounted for and inventoried. It is the intent of this policy to prevent devices and/or data from being deliberately or inadvertently stolen, improperly stored, and/or compromised in any manner.

2.0 SCOPE

This policy applies to all authorized system users. This includes DH, DHF, DoHS and OSA employees, business associates, contractors, and vendors who utilize either State-owned, company-owned, or personally-owned mobile devices to access, store, back-up, relocate, or access any State-provided resources or data.

This policy applies to any mobile device capable of storing State data and connecting to an unmanaged network. This includes, but may not be limited to the following:

- Laptops/notebooks
- Tablet computers such as iPads
- Cellular phones
- Smartphones
- Wireless routers

- Wireless network cards

This policy also applies to all wireless service and access, including, but not limited to, the following features:

- Voice
- Data
- Text Messaging
- Voicemail
- Caller ID
- Call waiting
- Call forwarding
- Three-way calling

3.0 POLICY

3.1 Access to State network resources is a privilege, not a right. Consequently, employment does not automatically guarantee the initial and ongoing ability to use mobile devices to gain access to State networks and information.

3.2 State-provided mobile devices may be provided to any Agency employee according to their job responsibilities and with management's approval.

3.3 Mobile devices are intended to provide the means to enhance the employee's ability to conduct State business.

3.4 Built-in configuration settings and security features of State-provided mobile devices will be standardized, documented, and implemented.

3.5 Employees should have no expectation of privacy regarding their use of wireless and/or mobile devices. The State reserves the right to monitor and/or review all

use on these devices for either operational or management purposes. This includes but is not limited to calls, voicemail messages, emails, text messages, etc.

3.6 Personal use of State-provided mobile and/or wireless devices and service is prohibited, except under certain circumstances, and must meet with the supervisor's approval. Personal use should only occur when it does **not** (1) interfere with the employee's work performance; (2) interfere with the work performance of others; (3) create undue impact on business operations; (4) incur incremental cost; or (5) violate any other provision of this policy or any other State or OMIS policy, procedure, or standard. (See WVOT policy WVOT-PO1002, *Acceptable Use of State-Issued Portable/Mobile Devices* for more information.)

3.7 All State-provided mobile and wireless devices connecting to the State network, or providing access to confidential information must:

- Adhere to the standards specified by the West Virginia Office of Technology (WVOT).
- Be installed, supported, and maintained by WVOT.
- Use WVOT-approved authentication protocols and infrastructure.
- Use WVOT-approved encryption protocols.
- Maintain a hardware address that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

3.8 Employee Responsibilities

3.8.1 All system users must comply with the guidelines set forth in WVOT policy WVOT-PO1002; as well as other applicable federal, state, and OMIS requirements, policies, and applicable contracts.

3.8.2 Employees must ensure that all State-provided mobile and wireless devices receive program updates, security patches, and anti-virus updates at intervals designated by the WVOT. (For more information, see WVOT-PO1002.)

3.8.3 Agency employees using mobile and wireless devices and related software for network and data access must utilize secure data management procedures. This includes confirming that password functionality is enabled on these devices and ensuring that strong password(s) are used, connecting to the State's Virtual Private Network (VPN), and using multi-factor authentication (MFA) for all accounts.

3.8.3.1 All passwords must conform to established standards designated by the WVOT Chief Information Officer (CIO)

3.8.3.2 When using MFA for any type of wireless or mobile device, employees may either register a State or personally owned smartphone for soft-token distribution or be assigned a hard-token (i.e. key fob). Those who have a State-issued cell phone, or access wv.gov email on a personal cell phone will not be approved for a key fob.

3.8.3.3 Users requesting a hard token for MFA must complete an MFA Hardware Token Request form at the following link: https://otsm.wv.gov/HEAT/Modules/SelfService/#serviceCatalog

3.8.4 Employees are prohibited from knowingly, willfully, and without authorization, directly or indirectly, tampering with, stealing, attempting to sell, altering, damaging, or destroying any State-provided mobile or wireless devices.

3.8.5 Employees are prohibited from intentionally removing or defacing State Asset ID Tags.

3.8.6 Mobile and wireless devices are classified as State property. Employees are responsible for proper safeguarding of their assigned device(s). Employees may be responsible for reimbursement to the Departments if improper or negligent care leads to damage or loss.

3.8.7 When an employee transfers from one bureau/office to another, his/her mobile and/or wireless device(s) must be cataloged and remain with the bureau/office responsible for purchasing the device(s).

3.8.8 Employees must contact an immediate supervisor if in doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding suspected theft or unacceptable use(s).

3.8.9 Employees will not use mobile devices (e.g., flash drives) as the primary storage location for any type of data. Data that is not currently in use, or critical user data needed for an extended period, must be backed-up to an alternate storage location or media.

3.8.10 Employees must take every precaution to ensure the privacy of confidential or sensitive information shown on the display or screen of a mobile or wireless device when in a public setting. If the employee cannot restrict this data from public view, the device must not be used.

3.8.11 Employees are responsible for the physical security of mobile and wireless devices in their care, and must take all reasonable precautions to prevent theft, vandalism, and/or the loss/disclosure of sensitive data. Employees are required to report lost or stolen devices immediately to WVOT's Online Computer Security and Privacy Incident Reporting System: https://apps.wv.gov/ot/ir/.

3.8.12 Employees must follow manufacturer's guidelines for the care and safe operation of their mobile and/or wireless devices.

3.9 DH, DHF, DoHS and the OSA Responsibilities

3.9.1 Agency supervisors are responsible for the following:

- Approving new wireless cellular service;
- Terminating or reassigning wireless cellular service;
- Recovering equipment or redistributing upon separation;
- Monitoring and tracking device usage and spending; and
- Adjusting service plans (as necessary) based on usage and spending.

3.9.2 Supervisors must establish and approve a need for an employee's use of standard cellular devices and/or service. Standard conditions are outlined in WVOT policy WVOT-PO1002.

3.9.3 OMIS will ensure that proper asset management procedures apply to all mobile devices.

3.9.4 Each bureau and office within DH, DHF, DoHS and the OSA must maintain an inventory of the mobile devices in service. This list will outline the following information:

- Device type;
- Serial Number;
- Person to whom the device is issued;
- Date of purchase;
- Warranty expiration; and

- Software installed.

3.9.5 When ordering a State-provided cell phone, Agency employees must follow procedures set forth in WVOTs *Mobile Device Management Procedures*, which applies to both agency-authorized personal devices and State-purchased devices. Each of these methods is provided to employees with the understanding that any device connected to the WVOT email system will be managed by WVOT. This document can be found at: https://westvirginiaot.sharepoint.com/sites/NAF/default.aspx.

3.9.6 Each bureau and office within DH, DHF, DoHS and the OSA must, on a quarterly basis, perform a review to ensure that all State-provided cell phones in their inventory are assigned to a current employee and being utilized on a regular basis.

3.10 WVOT Responsibilities

3.10.1 The WVOT will be responsible for loading mobile devices with a standard hardware and software configuration.

3.10.2 The WVOT will ensure that all mobile devices are encrypted, if technically possible.

3.10.3 All rules regarding the acceptable use of IT resources within State agencies apply to the use of mobile devices. For additional information, see policies WVOT-PO1001 and WVOT-PO1002.

3.10.4 All wireless access points and wireless devices connected to the State network must be registered and approved by WVOT. Wireless devices are subject to audits and penetration testing without notice.

3.10.5 The WVOT will negotiate contracts and monitor industry pricing plan changes, as well as update contracts for wireless service and mobile devices, as needed.

3.11 Access to and Use of Confidential Data

3.11.1 Federal Tax Information (FTI), Protected Health Information (PHI), Social Security Administration (SSA) data, Payment Card Industry (PCI) data, and Personally Identifiable Information (PII) should only be viewed or accessed on Agency-approved mobile devices.

3.11.2 FTI, PHI, SSA data, PCI data, and PII may be viewed and accessed on laptops only if approved by the bureau or office, and if those laptops are encrypted and connected to the State network.

3.11.3 VPN and MFA must be used on any devices accessing FTI, PHI, SSA data, PCI data, and/or PII.

3.12 Procurement

3.12.1 Services will not be authorized without a fully executed Agency Delivery Order (ADO).

3.12.2 The State is responsible for all procurement of State-provided mobile devices. It reserves the right to change service or plans at any time, for any reason.

3.12.3 All cellular services must be acquired through the statewide contract. Agencies are not authorized to create a separate contract(s) with cellular suppliers.

3.12.4 Wireless devices and/or services obtained independently from the statewide contract(s) will not be eligible for State reimbursement.

3.12.5 Office of Management Information Services (OMIS) approval is required for all new orders and/or reassignments of service based on established and objective needs criteria.

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

5.2 **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.

5.3 **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.

5.4 **Mobile Device** – A device made to be taken anywhere. Therefore, it needs an internal battery for power, and must be connected to a modern mobile network that can help it to send and receive data without attaching to a hardware infrastructure.

5.5 **Multi-Factor Authentication (MFA)** - Multi-factor authentication refers to the use of more than one of the following factors. The classic paradigm for authentication systems identifies three factors as the cornerstone of authentication:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a fingerprint or other biometric data)

The strength of authentication systems is largely determined by the number of factors incorporated by the system. Implementations that use two factors are considered to be stronger than those that use only one factor; systems that incorporate all three factors are stronger than systems that only incorporate two of the factors.

5.6 **Office of Management Information Services (OMIS)** – This office is part of the OSA, and reports directly to the DoH, DHF, and DHS Secretaries and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the Agencies.

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 the following:

- 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 **Virtual Private Network (VPN)** – A network that is constructed using public wires, usually the internet, to connect remote users or regional offices to a company's private, internal network.

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

5.12 **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.

5.13 **Wireless Device** – Any device that can communicate with other devices without being physically attached to them. Wireless devices do not have to be mobile, and most communicate through radio frequency.

6.0 REFERENCES/RELATED MATERIAL

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

6.2 WVOT-PO1001 – *Information Security Policy*

6.3 WVOT-PO1014 – *Malicious Software Protection*

6.4 OMIS Policy 0512 – *Information Security*

6.5 West Virginia Code §5A-6-4a – Powers and duties of the Chief Information Officer

6.6 West Virginia Code §61-3C-1 - West Virginia Computer Crime and Abuse Act, "Crimes and Their Punishment"

8.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	06/23/2016	Effective Date
Version 1.1	09/17/2018	Annual Review
Version 1.2	03/10/2020	Annual Review – revised sections 3.9, 3.12, and Section 6 (definitions) – added information re: VPN and MFA
Version 1.3	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)

OMIS Policy #0515 – Acceptable Use of Wireless and Mobile Devices

Revised: February 10, 2025

Version 1.4	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Annual review of content - Revised language throughout
Version 1.5	02/07/2023	Annual Review; Updated policy and WV Code links
Version 1.6	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 1.7	02/10/2025	Annual Review;overall review of content; minor language revisions throughout