State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services (OMIS)
Policy #0532: Wireless Access and Use

Revised: February 10, 2025

1.0 PURPOSE

The WV Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA), Office of Management Information Services (OMIS) provides wireless access at the One Davis Square (ODS) facility, which is available to users who have a need to access the Executive Branch network on a temporary basis.

This policy will establish the requirements and standards for use of the WV Public Access wireless network.

2.0 SCOPE

This policy applies to DH, DHF, DoHS and OSA employees, as well as all users of the WV Public Access wireless account provided by the State. This includes contractors, vendors, business associates, and federal partners.

3.0 POLICY

3.1 The WV Public Access wireless network is **provided for the temporary use of external contractors, vendors, business associates, and federal partners only.** (See OMIS Policy 0515, *Acceptable Use of Wireless and Mobile Devices* for more information.)

3.2 Users of the WV Public Access wireless are responsible for abiding by all applicable Departments' and Executive Branch policies, procedures, and guidelines.

3.3 OMIS takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by users, or for any data that may be lost or compromised while connected to the wireless network.

3.4 Wireless access will be provided at the discretion of OMIS. Users should have no expectation of privacy regarding their use of State-provided wireless.

3.5 OMIS reserves the right to disconnect any user at any time, for any reason. The WV Public Access wireless network is provided as a courtesy to allow guest access to the internet. Users will not be given access to the OMIS intranet or given permission to install any software on State-provided or personal devices (see West Virginia Office of Technology (WVOT) policy WVOT-PO1014, *Malicious Software Protection* for more information.).

3.6 Inappropriate use of the wireless is not permitted. This policy does not outline all possible inappropriate uses; however, it presents several guidelines that OMIS may, at any time, use to determine that a particular use is inappropriate (see Appendix "A" of WVOT-PO1001, *Information Security*, for more information):

- Users must respect the privacy and intellectual property rights of others.
- Users must respect the integrity of the State network and any other public or private computing and network systems.
- Use of the WV Public Access wireless network for malicious, fraudulent, or misrepresentative purposes is prohibited.
- The WV Public Access wireless network may not be used in a manner that prohibits or hampers other users' access to the wireless network or any other networks.
- Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.

3.7 All devices using WV Public Access wireless to connect to the State network, or provide access to confidential information must:

- Adhere to the standards specified by the WVOT and the Departments.
- Use WVOT-approved authentication protocols.
- 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 Use of the WV Public Access wireless to access, view, or transmit federal tax information (FTI), protected health information (PHI), social security administration (SSA) data, and personally identifiable information (PII) is strictly prohibited.

3.9 The State reserves the right to filter internet site availability, and monitor and review use as required for legal, audit, or legitimate authorized State operational or management purposes.

3.10 All individuals using the WV Public wireless network are responsible for the security of their device(s) and the data contained therein. Attempts to bypass security controls will result in the permanent loss of network access. Any device exhibiting behavior indicative of being compromised will be automatically removed from the network.

3.11 Individuals must not attach or use devices on the WV Public wireless network that are not authorized by OMIS or WVOT.

3.12 The unsecured nature and ease of connection to wireless hotspots increases the risk that unauthorized individuals can access a user's phone, laptop or other device, or communications over the wireless network. Users should take precautions to lower the security risks. For optimum security, authorized users must connect to the State network using VPN and multi-factor authentication (MFA). Users are encouraged to observe standard security practices by ensuring that computer hard drives are not shared; laptops have firewall protection; and security software is installed, functional, and updated on the device(s).

3.13 OMIS makes no representations or warranties concerning the availability or security of the WV Public Access wireless network, and all use is provided on an as-is basis. By using the WV Public wireless network, all users agree to defend, indemnify, and hold harmless the State of West Virginia and the DH, DHF, DoHS and OSA for any losses or damages that may result from use of the guest wireless network.

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, consultants, and/or federal partners 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 **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.

5.5 **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.

5.6 **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.

5.7 **Protected Health Information (PHI)** - A subset of PII and means, with regard to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered entities(see45 C.F.R. §106.103), individually identifiable health information, including demographic information, whether oral or recorded in any form or medium that relates to an individual's health, health care services and supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual including, but not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical

or mental condition, or functional status of an individual or that affects the structure or function of the body; or the past, present, or future payment for the provision of health care to an individual; and which includes identity information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected Health Information does not include records covered by the Family Educational Right and Privacy Act, 20 U.S.C. 1232g, and employment records held by the entity in its role as employer.

5.8 **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.

5.9 **Wireless Device** – Any device that can communicate with other devices without being physically attached to them. Most wireless devices communicate through radio frequency.

6.0 REFERENCES/RELATED MATERIAL

6.1 WVOT-PO1004 – *Acceptable Use of State-Issued Portable/Mobile Devices*

6.2 WVOT-PO1001 – *Information Security Policy*

6.3 WVOT-PO1014 – *Malicious Software/Anti-Virus*

6.4 OMIS Policy 0512 – *Information Security*

6.5 OMIS Policy 0515 – *Acceptable Use of Wireless and Mobile Devices*

6.6 West Virginia Code §5A-6-4a – "Duties of the Chief Information Officer Relating to Security of Government Information"

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	02/06/2019	Initial Version
Version 1.2	03/19/2020	Annual Review
Version 1.3	03/25/2021	Annual Review
Version 1.4	02/01/2022	Converted document from Word to Google Docs; Updated formatting; Overall review of content - Revised language throughout
Version 1.5	02/07/2023	Annual Review; updated policy 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 2.0	02/10/2025	Annual review; overall content, link, and format review