State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0522 - Account Access

Revised: February 10, 2025

1.0 PURPOSE

The purpose of this policy is to establish uniform security requirements, and to define standards for all authorized users who require access to the Executive Branch network and any information assets received, created, maintained, or transmitted by the State. This may include networks; systems; applications; and protected information including but not limited to electronic protected health information (e-PHI), personally identifiable information, (PII), Social Security Administration (SSA) data, payment card industry (PCI) data, and federal tax information (FTI). The guidelines set forth in this policy are designed to minimize exposure and damages that may result from unauthorized access and use of State resources and protected information.

Network account access is a privilege and is granted only to users who have a business defined need and meet the eligibility requirements of the WV Executive Branch and Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) policies and procedures, and who demonstrate compliance with established safeguards protecting the confidentiality, integrity, and availability of information resources.

2.0 SCOPE

This policy applies to all authorized system users within the WV DH, DHF, DoHS, and the OSA. This policy also applies to external entities including business associates, contractors, and vendors who require connectivity to the State network, systems, applications, and data. Users are frequently categorized in one of the following user groups:

1. Employees with permanent access. These users are often Information Technology (IT), executive management, teleworkers, or designated employees who require 24-hour system availability and are often called upon to work remotely or who travel often. Their remote access offers the same level of access as their on-site access and requires the use of state equipment, state approved and installed image, device encryption, secure connection (usually via secured VPN) and multifactor authentication.

2. Employees with temporary access. These users typically require short-term access due to a temporary State position or temporary contractor or vendor status. These users are treated as if they were permanent access employees with all privacy and security requirements.

3. Contractors, vendors, and other business associates offering product support with no access to protected information. These users have varied access depending upon the systems needed for application or system support, but do not have access to any PHI, PII, FTI, PCI, or SSA data in the applications or systems. These users access the system on an as needed basis for system troubleshooting and require the use of state equipment, state approved and installed image, device encryption, secure connection (usually via secured VPN) and multifactor authentication.

4. Contractors and vendors offering product support and other business associates with access to protected information. These users have varied access to protected information depending on the application or system supported and/or accessed. WV State Code 15-2D-3 requires any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background check. Appropriate Memorandums of Understanding (MOU), Data Use Agreements (DUA), Business Associate Agreements (BAA), and/or applicable contracts must be on file prior to allowing access, and all such access must be audited on a regular basis. These users require the use of state equipment, state approved and installed image, device encryption, secure connection (usually via secured VPN) and multifactor authentication.

5. Teleworkers are employees who, for at least one or more days within a week, work at home or an alternate worksite. Contractors or vendors may also have remote access privileges for emergency and disaster recovery purposes. Access for these users is typically restricted to only that which is necessary for task completion during the time away from the office and may be limited to specific application access only. Remote access requires telework approval, secured connection, and multifactor authentication to access the State's network. These users require the use of state equipment, state approved and installed image, device encryption, and secure connection (via secured VPN). For additional information see the Departments of Health,

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0522 - Account Access

Revised: February 10, 2025

Health Facilities, and Human Services Policy 2122, *Extenuating Circumstances Telework Policy*

3.0 POLICY

3.1 Employee Network Access

3.1.1 The West Virginia Office of Technology (WVOT) has established standards for creating, issuing, removing, monitoring, and managing all Executive Branch employee network accounts.

3.1.2 Network user accounts will not be activated until accompanied by written and authorized documentation (Network Logon Request Form).

3.1.3 DH, DHF, DoHS, and OSA bureaus and offices will appoint one or more employee(s) to act as a designated approval authority (DAA). This individual(s) will authorize all network account modifications for that bureau/office.

3.1.4 The Office of Management Information Services (OMIS) will work with 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. The WVOT reserves the right to audit all agency accounts, as necessary.

3.1.5 For more information on network account access, see WVOT Policy WVOT-PO-1021, *Account Management.*

3.2 Remote Access

3.2.1 Remote access must only be used for legitimate business purposes.

Revised: February 10, 2025

3.2.2 Remote access requires authentication and authorization to access needed resources, and access rights will be regularly reviewed. Employees must use the statewide authentication and authorization service managed by WVOT.

3.2.3 Each user who accesses the network remotely will be uniquely identifiable. Account passwords will not traverse the network in clear text and must meet the minimum requirements of the Executive Branch password management standards.

3.2.4 All individuals requesting a remote access connection must apply by completing an online Remote Access Request form at the following link: (https://sites.google.com/wv.gov/ivantiselfservice?pli=1). Remote access is strictly controlled and made available only to those employees, contractors, and/or vendors,

at the discretion of the employee or contractor manager, and with approval by a bureau or office DAA.

3.2.5 Remote access will not be activated until the authorization process and the required documentation are completed. Once a user gets remote access, that user must then obtain VPN access by installing the software if it was not installed during the state imaging process. (Directions may be found at the following link: (https://sites.google.com/wv.gov/ivantiselfservice?pli=1)

3.2.6 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 the devices and ensuring that strong passwords are used.

3.2.7 All devices connecting to the State network remotely must be configured with a current operating system, device appropriate encryption, up-to-date antivirus software, secure tunneling software, and current patch updates.

Revised: February 10, 2025

3.2.8 When accessing the network remotely, all devices must be connected to the State's VPN and multi-factor authentication (MFA) must be used for all accounts.

3.2.8.1 By employing MFA, users may access the system by registering a State or personally-owned smartphone for soft-token distribution or be assigned a hard-token (i.e. key fob).

3.2.8.2 Users employing a hard token for MFA must submit an MFA Hardware Token Request at the following link: https://otsm.wv.gov/HEAT/Modules/SelfService/#serviceCatalog. Users who have a State-issued cell phone or who utilize wv.gov email on their personal cell phone will not be approved for a hardware token.

3.2.9 Remote users must not engage in illegal activities and must refrain from using remote access for interests other than those of the DH, DHF, DoHS and the OSA. Users must not access, receive, process, store, transmit, or dispose of FTI in IT systems located offshore.

3.2.10 WVOT is responsible for establishing and documenting usage restrictions, outlining configuration/connection requirements, and monitoring for unauthorized remote access to the information system. See sections 3.1, 3.2, and 3.7.4 of WVOT Policy PO1001, *Information Security*, for more information.

3.2.11 Business associates, contractors, and vendors may be granted remote access to the State network, provided they have an MOU, a contract, or other agreement with the State or the DH, DHF, DoHS and/or the OSA. Agreements must clearly define the type of remote access permitted (i.e., stand-alone host, network server, etc.), as well as other conditions required, such as MFA, virus protection software, device encryption and VPN connection. Such contractual provisions must be reviewed and approved by the OMIS Chief Information Officer (CIO) and the WVOT before remote access will be permitted.

3.2.12 All users granted remote access privileges must sign and comply with the WV Executive Branch Confidentiality Agreement and the DH, DHF, DoHS, and OSA Employee or

Vendor Confidentiality Agreement, as applicable. This document must be signed annually, or when terms/conditions changes are necessary, and will be kept on file with each Department's Human Resources office.

3.2.13 Employees utilizing remote access for telework must complete telework requests and all documentation for approval by their immediate supervisor. Employees who telework on an occasional basis must obtain approval from their immediate supervisor at least 24 hours in advance.

3.2.14 It is the remote user's responsibility to ensure the remote worksite meets security and configuration standards established by the Executive Branch and the DH, DHF, DoHS, and OSA policy and procedure. This includes VPN and MFA requirements, configuration of equipment, of personal routers and wireless networks, and workspace accommodations as addressed in *Departments of Health, Health Facilities, and Human Services Extenuating Circumstances Telework Policy 2122*.

3.3 Temporary Network Accounts

3.3.1 Temporary accounts will be approved on a need-to-use basis following the principle of least privilege.

3.3.2 Temporary accounts will expire within 365 days or at the time of the work completion date, whichever occurs first.

3.3.3 All temporary accounts must be verified by an authorized member of the DH, DHF, DoHS, and OSA.

3.3.4 All temporary accounts must be specifically identified at the time of the network access request, so the individual will not be mistaken for a full-time State employee.

3.4 Guest Wireless Accounts

3.4.1 OMIS guest wireless access is provided for the temporary use of external contractors, vendors, business associates, and federal partners only. Guest wireless must not be accessed and/or used by Department employees under any circumstances.

3.4.2 For more information re: OMIS guest wireless access, see OMIS Policy #0532, *Wireless Access and Use.*

3.5 Security and Privacy

3.5.1 Only authorized users are permitted access to State of WV computer systems, computer networks, and/or data. Users must adhere to all applicable state and federal information security and privacy requirements and policies.

3.5.2 Any remote connection to protected information (e-PHI, PII, SSA, PCI, and FTI) must be established using secured access and MFA.

3.5.3 All users, including employees, business associates, contractors, and vendors must log off and disconnect from the network when accessing remotely.

3.5.4 Users must lock their workstations when left unattended so no other individual may access the State network and/or confidential/protected information.

3.5.5 Remote users will be automatically disconnected from the network when there is no recognized activity for 15 minutes.

3.5.6 Users must not provide their username or password to anyone under any circumstances.

3.5.7 All users must take necessary precautions to secure all State-owned equipment and proprietary information in their possession.

3.5.8 Virus protection software is installed by WVOT on all State-owned computers and is set to update whenever new definitions are available (see WVOT-PO1014 – *Malicious Software Protection*). This update is critical to the security of all data, and users must not stop the update process for virus protection on the workstation.

3.5.9 Firewall software on computers and device appropriate encryption must be used and may not be disabled for any reason.

3.5.10 Users are required to encrypt protected information when sending through email. All methods of encryption utilized during remote access must comply with WVOT encryption standards. (For more information, contact the WVOT Service Desk at servicedesk@wv.gov or 304-558-9966.)

3.5.11 Unless authorized by the OMIS Information Security Officer (ISO), copying of confidential/protected information to external media and mobile devices (hard drives, USB devices, CDs, etc.) is strictly prohibited.

3.5.12 WVOT maintains audit logs of all activities performed by users while connected to the network whether working on site or from remote locations. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity. Accounts that have shown no activity for 60 days will be disabled.

3.5.13 Reconfiguration of non-State equipment for the purpose of split-tunneling or dual homing is not permitted at any time and is considered a security breach.

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.

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0522 - Account Access

Revised: February 10, 2025

5.0 DEFINITIONS

5.1 **Business Associate Agreement** - A contract between a HIPAA covered entity and a HIPAA business associate (BA) that is used to protect PHI in accordance with HIPAA guidelines. Under the U.S. Health Insurance Portability and Accountability Act of 1996, a HIPAA business associate agreement (BAA) is a contract between a HIPAA covered entity and a HIPAA BA. The contract protects PHI in accordance with HIPAA guidelines.

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

5.3 **Data Use Agreement (DUA)** – A legal binding agreement required when transferring a "limited data set" from one entity to another. A DUA serves as both a means of informing data users of their requirements and a means of obtaining the agreement to abide by these requirements. The DUA also serves as a control mechanism for tracking the location(s) of the organization's data and the reason for the release of the data.

5.4 **Electronic Protected Health Information (e-PHI)** - Individually identifiable health information that is electronically and digitally 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.

5.5 **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 DH, DHF, DoHS and the OSA to be subject to this policy. This definition does not create any additional rights or duties.

5.6 **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.

5.7 **Firewalls** - A logical or physical discontinuity in a network to prevent unauthorized access to data or resources. A firewall is a set of hardware and/or related programs providing protection from attacks, probes, scans and unauthorized access by separating the internal network from the Internet.

5.8 **Information Resources** - Networks, systems, applications, and data including but not limited to, PHI received, created, maintained or transmitted by the DH, DHF, DoHS and the OSA.

5.9 **Memorandum of Understanding (MOU)** – Describes a bilateral or multilateral agreement between two or more parties. It expresses a merging of will between the parties, indicating an intended common line of action. It is often used in cases where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement.

5.10 **Multi-Factor Authentication** - 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.

5.11 **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.

5.12 **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.

5.13 **Protected Information** – any information that is protected by federal or state regulations, such as federal tax information, social security information, and health information. This also includes business proprietary information, sensitive and confidential information and any information that is defined in the WVOT policy WVOT-PO1006, Data Classification.

5.14 **Remote Access** - The ability to gain access to the State's network from outside the network perimeter. Common methods of communication from the remote computer to the network

include, but are not limited to, VPN, web-based Secure Socket Layer (SSL) portals, and other methods which employ encrypted communication technologies.

5.15 **Role-Based Access** - Access control mechanisms based on predefined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned a predefined role based on the least-privilege principle.

5.16 **Scan** – To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices (e.g., changes to an executable file, direct writes to specific disk sectors, et. al.).

5.17 **Split-tunneling** - Simultaneous direct access to a non-State network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into a trusted administrative network via a VPN tunnel.

5.18 **Teleworker** - An employee who, for at least one or more days within a week, works at home or at an alternate worksite, to produce an agreed upon work product.

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

5.20 **Virtual Private Network (VPN)** - An encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

6.0 REFERENCES/RELATED MATERIAL

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

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0522 - Account Access

Revised: February 10, 2025

6.2 WVOT – PO1001 – Information Security Policy

6.3 WVOT – PO1002 – Acceptable Use of State Issued Portable/Mobile Devices

6.4 WVOT – PO1014 – Malicious Software/Anti-Virus

6.5 WVOT – PO1012 – Contractor Management

6.6 WVOT – PO1006 – Data Classification

6.7 WVOT – PO1005 – Email Use Standards

6.8 WVOT – PO1022 – Acceptable Internet Usage

6.9 WVOT – PO1011 – Digital Media Protection

6.10 WVOT – PO1021 – Account Management

6.11 Departments of Health, Health Facilities, and Human Services – Policy Memorandum 2122 – Extenuating Circumstances Telework Policy

6.12 Office of Management Information Services (OMIS) Policy 0512 – Information Security

6.13 Office of Management Information Services Policy 0510 – Email Guidelines and Requirements

State of West Virginia
Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0522 - Account Access

Revised: February 10, 2025

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	02/06/2019	Original
Version 2.0	03/19/2020	Updated language in section 3.2.6
Version 2.1	03/25/2021	Updated language in sections 3.2.6 and 3.5
Version 2.2	02/01/2022	Converted document from Word to Google Docs, Updated formatting,Overall review of content - Revised language throughout
Version 2.3	02/07/2023	Removed reference to OMIS Telework policy in No. 5 in Scope, updated links to WVOT and DHHR policies and network access forms
Version 2.4	01/08/2024	Annual Update - changed “DHHR” to “Departments of Health, Health Facilities, Human Services, and Office of

Revised: February 10, 2025

		Shared Administration", updated links, overall review of content, revised language throughout
Version 2.5	02/10/2025	Annual Review – minor revisions to language and format