State of West Virginia Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0535 – Collaborative Computing

Revised: January 26, 2026

1.0 PURPOSE

Collaborative computing allows people in geographically distant locations to work together on a project. It takes many forms and includes groupware, instant messaging (IM), web conferencing, email, calendaring, and other technologies. The key component is that two or more individuals share a resource so they can work together.

1.1 Collaborative Computing is useful, but it presents certain risks. These may include the following:

- Malware – Viruses, spyware, Trojans, and worms transferred through instant message sessions and peer-to-peer data exchanges.
- Loss of Data Confidentiality – Data transferred via a collaborative software tool is subject to unauthorized disclosure at several points during the communication session. The traffic generally passes through third-party networks and servers out of the control of the data owner.
- Network Attacks – Collaborative software tools open additional network ports creating a larger attack surface and more entry points for untrusted users to launch denial of service, spamming and man-in-the-middle attacks. Also, these tools use excessive amounts of network bandwidth creating the potential for unintended denial of service.

1.2 In addition to these risks, collaborative computing presents an opportunity for remote users to listen in or watch local activities through computer-based microphones and cameras that have not been properly turned off.

This policy is an attempt to mitigate these risks to protect the State of West Virginia systems, data, and confidentiality.

State of West Virginia Departments of Health, Health Facilities, and Human Services
Office of Shared Administration
Office of Management Information Services
Policy 0535 – Collaborative Computing

Revised: January 26, 2026

2.0 SCOPE

This policy applies to all State of West Virginia Departments of Health (DH), Health Facilities (DHF), Human Services (DoHS), and Office of Shared Administration (OSA) (Departments) employees as well as independent contractors, business associates, vendors, and third-party contractors regardless of classification, rank, or seniority.

The intent of this policy is to explain the range of acceptable and unacceptable uses of Collaborative Computing resources and is not necessarily all-inclusive. This requirement applies to all agency IT resources and assets used by the agency that process, store, transmit or secure sensitive or confidential data, including those provided by contractor support.

3.0 POLICY

3.1 Unless explicitly authorized in writing by the Office of Management Information Services (OMIS) Chief Information Officer (CIO) or a designated representative, collaborative computing is prohibited in order to protect State systems, data, and confidentiality. (For a detailed description of protecting State systems, data, and confidentiality see OMIS Policy #0524: *Workstation Security* and OMIS Policy #0512: *Information Security*.)

3.2 The following activities have been authorized by the CIO:

3.2.1 State-provided email allows employees to send and receive email for collaborative information sharing.

3.2.2 State-provided email calendar application allows employees to share calendars for collaborative scheduling.

3.2.3 State-provided instant messaging (IM), chat, and web conferencing allow employees to conduct conference calls and instant messaging.

3.2.3.1 During a web conferencing session, data confidentiality must be observed. For example, users should not share sensitive and/or confidential data {i.e., protected health information (PHI), personally identifiable information (PII), federal tax information (FTI), social security administration data (SSA), and/or payment card information (PCI)} with individuals who are not authorized to see it. Users must not leave data files open on their desktops during a web conferencing session. (See OMIS Policy #0524 for more information.)

3.2.3.2 Employees are prohibited from downloading and using personal, consumer-grade IM or chat software to transmit messages. (See section 3.2 of WVOT Policy #PO1010 *Acceptable Use of Instant Messaging* for information.)

3.2.4 Electronic White Boards may be utilized as a collaborative computing tool. However, users must adhere to all requirements outlined in this policy.

3.3 When utilizing collaborative computing devices, the following conditions must be met:

3.3.1 The information system must prohibit remote activation of collaborative computing devices, i.e., the system must not allow a remote user to turn on a camera or microphone on a local device.

3.3.2 The information system must provide an explicit indication of use to users physically present at the device, i.e., the system must indicate to local users that

resources are being shared with remote users (e.g., flashing a warning on the screen).

3.3.3 In lieu of using a collaborative software tool such as GoToMeeting or GoToAssist to transmit confidential or sensitive data, employees must use agency-controlled Virtual Private Networks (VPNs) that provide FIPS 140- 2 or greater compliant cryptography to prevent a loss of data confidentiality and/or integrity.

3.4 Departments' employees should have no expectation of privacy when using State-provided resources for collaborative computing.

3.5 Cloud Computing

3.5.1 As part of its duty of care to employees and customers, and as a matter of good business practice, the confidentiality, integrity and availability of all IT applications, data, systems, and network resources implemented in the State's Cloud environment must be managed by a formal information security management program. This program will provide a controlled and logical method by which access to cloud-based information systems is requested and granted, security of cloud-based systems and data is monitored and analyzed, violations of cloud security are addressed and mitigated, and changes to cloud security systems and procedures are requested, tested, approved, and communicated for auditing purposes.

3.5.2 WVOT will define cloud security processes and procedures; secure and utilize specialized software and systems to reduce the threat of cloud security breaches; regularly test the security of State network perimeters and the cloud service

vendor's perimeters using penetration tests and other forensic methods; and document all information cloud procedures and controls.

3.5.3 WVOT will periodically conduct a risk assessment of the internal and external threats and vulnerabilities of the State network.

3.5.4 WVOT will manage cloud security policy for the State and will ensure that the cloud service provider (CSP) adopts and adheres to all applicable state and federal cloud security requirements, policies, and procedures.

3.6 Use of Collaborative Computing in an FTI Environment

3.6.1 In order to minimize improper access or disclosure, access to collaborative tools and applications will be limited to authorized personnel with a need to know.

3.6.2 Privileged and non-privileged account users must utilize multifactor authentication (MFA) for remote network access to information systems that process, store, transmit, are used to access, and/or used to protect FTI. This includes but is not limited to remote access from FTI system administrators who may be accessing operating systems, databases, management interfaces, or other system components from a non-agency location (e.g., working remote locations).

3.6.3 State systems must meet NIST Special Publication 800-63B requirements, Authenticator Assurance Level 2 (AAL2), for an MFA solution to be considered sufficient.

3.6.4 When an MFA authenticator is used, any of the following may be used:

- A one-time-password (OTP) device (i.e., a fob that receives a time-bound secret combined with a known PIN or biometrics)
- Cryptographic software (i.e., a software-based solution that captures one or more secret keys unique to the authenticator which are only accessible through the input of an additional factor, such as a PIN or biometrics)
- Cryptographic device (i.e., a hardware-based solution that captures one or more secret keys unique to the authenticator which are accessible only through the input of an additional factor, such as a PIN or biometrics)

3.6.5 FTI cannot be accessed remotely by agency employees, agents, representatives, or contractors located offshore, i.e., outside of the United States territories, embassies, or military installations.

3.6.6 FTI may not be received, processed, stored, transmitted, accessed by or through, and/or disposed of by IT systems located offshore.

3.6.7 In order to manage the flow of FTI, access controls will be established so that only individuals who have identification and authentication credentials can see the data in the collaborative computing tool.

3.6.7.1 System event logs will be utilized to track individual access to FTI.

3.6.7.2 The DH, DHF, DoHS, and the OSA will ensure that any non-disclosure or confidentiality agreements with third parties, contractors, and other partners include specific mention of information held in the agency collaboration tools and applications.

Revised: January 26, 2026

3.6.8 Remote Activation/Teleworking

3.6.8.1 The DH, DHF, DoHS, and the OSA will collaborate with WVOT and third-party contractors, as needed, to:

3.6.8.1.1 Establish and document usage restrictions, configuration and/or connection requirements, and implementation guidance for each type of remote access allowed.

3.6.8.1.2 Authorize remote access to the information system prior to allowing any connections.

3.6.8.1.3 Authorize and document the execution of privileged commands and access to security-relevant information via remote access for compelling operational needs only.

3.6.8.2 Examples of network and remote access include, but are not limited to, the following:

- Remote access from application front-end users who may be accessing confidential or sensitive data through application interfaces from a non-agency location (i.e., working from home).
- Remote access from system administrators who may be accessing operating systems, databases, or other system components from a non-agency location.

- Remote access from IT staff who may be administering network protection equipment from a non-agency location, even if those system administrators do not have logical access to confidential data.
- Administrative users logged-in to the management interface of one of the devices under their control (i.e., firewall, router, server operating system, etc.) from their workstation.
- Access from third-party contractors to front-end systems when those connections do not leverage private circuits or direct network connections (i.e., using a site-to-site VPN tunnel).

3.6.8.3 DH, DHF, DoHS, and the OSA employees accessing confidential data or systems may work from home or other approved sites only if the confidentiality of PII, PHI, FTI, SSA data, and/or PCI data can be adequately protected at the highest level of attainable security. All required physical protections for computers, electronic devices, and media, apply to telework locations and collaborative technologies used to facilitate remote access and telework capabilities.

3.6.8.4 State-owned computers and devices must be used when establishing remote connections to State-managed remote access solutions (e.g., VPN)

3.6.8.5 The WVOT will configure its technological systems (e.g., VPN) to:

- Monitor and control remote access methods.

- Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions that transmit FTI over the remote connection.
- Route all remote access through a limited number of managed network access control points.

3.6.8.6 Bureaus and offices accessing PII, PHI, FTI, SSA, and PCI data must remove or disable networked white boards, cameras, microphones, and other technologies supporting remote viewing, downloading, and read and write functions from systems that process, store, and transmit the confidential data.

3.6.8.7 When using a collaborative computing device, users must ensure it provides an indication such as activity light or event notifications when activated.

3.6.8.8 Remote Desktop connections are only permitted when interacting with WVOT.

3.6.8.9 Any remote access where confidential data is accessed over a remote connection must be performed using MFA.

3.7 Security Requirements

3.7.1 The following is a list of requirements for users and administrators to best protect confidential data and systems:

Revised: January 26, 2026

3.7.1.1 The agency must retain ownership and control, for all hardware, software, and end-point equipment connecting to public communications networks. No unauthorized software will be installed on State systems.

3.7.1.2 Employees must take every precaution to ensure the privacy of confidential or sensitive information shown on the display or screen of laptops, tablets, and phones when in a public setting. If the employee cannot restrict this data from public view, the device must not be used. (For more information, see OMIS Policy #0515, *Acceptable Use of Wireless and Mobile Devices*).

3.7.1.3 Employees must utilize encryption by establishing VPN tunnels using FIPS compliant algorithms, before accessing confidential data and systems.

3.7.1.4 Employees must always implement a session lock on their State provided laptop when walking away from the device either at work or at a telework location.

3.7.1.5 Employees will create strong passwords that must conform to federal and WVOT-designated standards.

3.7.1.6 Employees will log out of interactive sessions when no longer needed.

3.7.1.7 Employees are prohibited from sending email containing FTI through the Executive Branch email system, either in the body of an

email or as an attachment (see OMIS policy #0510, *Email Requirements*, for more information).

3.7.1.8 In order to effectively safeguard confidential information, and to ensure the security and integrity of the information contained within the State network, all email messages and attachments containing sensitive and/or confidential information must be encrypted in transit.

3.7.1.9 Any employee who releases sensitive or confidential information through State-provided email, whether intentional or unintentional, may be subject to disciplinary action according to applicable state and federal laws and Executive Branch rules, policies, and procedures regarding confidentiality.

3.7.1.10 The Departments will provide employees, or ensure they possess, locking file cabinets or desk drawers so documents and electronic media containing confidential data may be properly secured when not in use.

3.7.1.11 Users will be provided "locking hardware," such as cable locks, to secure automated data processing equipment (for example, laptops) to large objects such as desks or furniture. In the absence of locking hardware, equipment must be locked in a filing cabinet or desk drawer when not in use, including temporary absences.

3.7.1.12 FTI may be stored on hard disks only if WVOT-approved security access control devices (hardware/software) have been installed and

are receiving regularly scheduled patches and/or updates. Access control must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

3.7.1.13 Employees must use only WVOT-approved security access control devices and/or software when establishing remote connections. This includes connecting to the State's VPN and using MFA for all accounts (See OMIS Policy #0522, *Account Access*, for more information).

3.7.1.14 WVOT and the OMIS will provide users with specialized training in information security, privacy, and disclosure awareness. All employees must complete mandatory online information security and privacy awareness training annually.

3.7.1.14.1 Employees with assigned security roles and responsibilities will receive role-based security training prior to receiving access to the information system or performing duties requiring access to FTI, when required by information system changes, and at least annually thereafter.

3.7.1.15 The DH, DHF, DoHS, and the OSA will establish, implement, and maintain a policy for the security of alternative work sites.

3.7.1.15.1 OMIS will coordinate with WVOT to ensure that all security controls are adequate for security needs.

3.7.1.15.2 OMIS will disseminate policies and procedures to ensure that teleworkers do not leave computers unprotected at any time, and establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.

4.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action will be administered by the employing agency and may be based upon recommendations of WVOT and the West Virginia Division of Personnel.

5.0 DEFINITIONS

5.1 Cloud Computing – A model for enabling universal, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

5.2 Collaborative Computing – Technology that allows people in geographically distant locations to work together on a project.

5.3 Confidentiality – A policy of protecting the personally identifying information (PII) of individuals and keeping it out of the hands of unauthorized people.

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

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 WVOT to be subject to this policy. This definition does not create any additional rights or duties.

5.6 Federal Tax Information (FTI) – According to 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 Malware – Software such as viruses and spyware that is intended to do harm or collect information.

5.8 Network Attack – Penetration of a network system by hackers with the intent of breaking through defenses such as firewalls for the purpose of doing harm or collecting information.

5.9 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.

Revised: January 26, 2026

5.10 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.

5.11 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.

5.12 Remote access - Any access to an agency information system by a user communicating through an external network, for example, the Internet.

5.13 Remote Desktop Connection – An application that allows authorized remote users, such as WVOT technicians, to access a local computer for the purpose of correcting a problem, adding a feature such as a new printer, or installing software.

5.14 White Board – A wall-mounted, interactive device that allows you to share information with others locally and remotely.

6.0 REFERENCES/RELATED MATERIAL

6.1 Internal Revenue Service (IRS) Office of Safeguards *Use of Collaborative Computing Devices*

6.2 Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Controls for Affordable Care Act (ACA), Medicaid, and Partner Entities (ARC-AMPE), version 1.02, April 10, 2025 - SC-15: *Collaborative Computing Device*

6.3 WVOT-PO1006 – *Data Classification policy*

6.4 WVOT Policy #PO1010 - *Acceptable Use of Instant Messaging*

6.5 OMIS policy #0510, *Email Requirements*

6.6 OMIS Policy #0512 - *Information Security Policy*

Revised: January 26, 2026

6.7 OMIS Policy #0515, *Acceptable Use of Wireless and Mobile Devices*

6.8 OMIS Policy #0522, *Account Access*

6.9 OMIS Policy #0524 - *Workstation Security*

7.0 REVISION HISTORY

Version Number	Date	Revisions
Version 1.0	06/30/2022	Initial Version
Version 1.1	02/07/2023	Overall review of content; updated policy links
Version 1.2	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 1.3	02/10/2025	Annual revisions and update - reviewed links and language; reformatted font
Version 1.4	01/26/2026	Annual review and update - reviewed and updated links, language, and format