

Doc. #	Policy Information
PO1010	<p><u>Acceptable Use of State-Provided Instant Messaging</u> Summary: This policy Outline the applicable rules applied when using the State-provided system. Edits: Added History Change Log; Inserted Section 4.11, “While using the State’s Instant Messaging product, employees must follow all applicable policies provided by the Division of Personnel, as well as any agency-specific policies related to employee communication.”</p>
PO1002	<p><u>Acceptable Use of State-Provided Wireless Devices</u> Summary: This policy establishes a framework for the procurement, possession, and appropriate use of West Virginia state-owned and/or paid wireless communication equipment and/or services. In addition, all rules regarding the acceptable use of IT resources within State agencies apply to the utilization of portable devices. Edits: Modified section 4.1.2, changed “department” to “agency”; Added Change Log History</p>
PO1021	<p><u>Account Management</u> Summary: This policy outlines the standards for creating, issuing, removing, monitoring, and managing employee accounts. Edits: Added Change Log History; Changed Section 4.1 to read, “The WVOT is responsible for adding, modifying, and deleting network users’ account access for Executive Branch agencies. Name changes, accounting changes, and permission changes are all documented.”; Deleted repetitive Section 4.5, “The use of shared accounts is prohibited, unless authorized by the WVOT. Each account must have a designated owner who is responsible for the management of access to that account and for maintaining a list of individuals who have access to the shared account.”</p>
PO1025	<p><u>Accreditation and Certification</u> Summary: This policy is outlines how the West Virginia Office of Technology (WVOT) validates the security readiness for devices, systems, application and system software, and other technology prior to deployment into a production status. Edits: Added Change Log History; Added Appendices A and B; Clarified and reorganized sections on Phase I and Phase II.</p>
PO1014	<p><u>Anti-Virus / Malicious Software</u> Summary: This policy describes prescribes the measures required to counter computer viruses, malicious code, and other malware. It identifies responsibilities in protecting the State network against malicious software. Edits: Added Change Log History; Changed Policy name from “Anti-Virus” to “Malicious Software Protection”; Added Sections 4.9 through 4.12; 4.9) Scans of computers and systems will be performed weekly, at a minimum. 4.10) Real-time scans must be performed on files from external sources that are downloaded, opened, or executed in accordance with agency security policy. 4.11) Malicious code and software will be blocked or quarantined. 4.12) WVOT will manage malicious code protection mechanisms and automatically update these protection mechanisms as needed.</p>
PO1008	<p><u>Auditing Program</u> Summary: The West Virginia Office of Technology (WVOT) will maintain an objective and internally independent Information Security Audit Program. This program will serve the Executive Branch by examining, evaluating, and reporting on information technology (IT) applications, related systems, operations, processes, and practices to provide reasonable assurance security controls. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>

Doc. #	Policy Information
PO1015	<p><u>Change and Configuration Management</u> Summary: The purpose of Enterprise Change Management is to standardize the identification, evaluation, planning, coordination, communication and implementation of changes to the State computing environment in such a way as to minimize any potential disruption to the user community, to ensure that all impacted users and support groups are making necessary accommodations to the change(s), and to increase the value of Information Resources. Edits: New!</p>
PO1012	<p><u>Contractor Management</u> Summary: This policy provides standard methodology to help manage the activities surrounding the engagement and termination of contractor services in the IT environment for the State. Edits: Added Change Log History</p>
PO1013	<p><u>Data Backup and Retention</u> Summary: This policy outlines data backup requirements for the West Virginia Office of Technology (WVOT) to ensure availability of critical data and systems within Executive Branch agencies. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1006	<p><u>Data Classification</u> Summary: This policy presents the framework through which all State of West Virginia (State) government agencies, employees, vendors, and business associates, specifically those in the Executive Branch, must classify their data and systems, as they relate to (1) data sensitivity; and (2) data and system criticality Edits: Added Change Log History; Added Section 4.6.2.4: To utilize a cloud computing services to receive, transmit, store, or process Very Sensitive information, the agency must ensure: 1) Data is isolated. Software, data, and services that receive, transmit, process, or store sensitive State data must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications; 2) A Service Level Agreements (SLA) is in place between WVOT and the Agency; 3) Data is encrypted during transit. Sensitive data must be encrypted in transit within the cloud environment. All mechanisms used to encrypt the data must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module; 4) Data is encrypted at rest in the cloud; 5) Devices accessing the cloud storage can be securely sanitized and/or destroyed at the end of their life cycle or if the device is lost or stolen; 6) They assess, annually, the security controls in place on all information systems used for receiving, processing, storing and transmitting the sensitive information stored in the cloud; and 7) Security controls must be identified, documented and implemented.</p>
PO1005	<p><u>Email Use Standards</u> Summary: This policy establishes and communicates the acceptable use of, access to, and disclosure of the State-provided e-mail system. Edits: Added Change Log History</p>
PO1023	<p><u>E-Recycling/End of Life</u> Summary: This policy directs technology-related inventory from assessment prior to potential reuse, through final disposition. Edits: Defunct</p>
PO1001	<p><u>Information Security Policy</u> Summary: The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources Edits: Added Change Log History; Split Section 4.5 into two sections, 4.5 and 4.6, respectively. Modified 4.6 to begin "Agencies are required to have employees sign..."</p>

Doc. #	Policy Information
PO1022	<p><u>Internet Use</u> Summary: The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided internet access and is not necessarily all-inclusive. Questions about specific internet uses which are not detailed in this policy should be directed to an agency supervisor or manager. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1011	<p><u>Media Protection</u> Summary: This policy defines standards, procedures, and restrictions for Executive Branch employees who use authorized removable media to connect to any device attached to a WVOT-supported network, in order to store, back-up, relocate, or otherwise access enterprise data in a safe, secure manner. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1018	<p><u>Network Violation Reporting</u> Summary: The purpose of this policy is to outline the courses of action prescribed for both the West Virginia Office of Technology (WVOT) and Executive Branch agencies when network violations are detected on the State network. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PR1017	<p><u>Password Standards Procedure</u> Summary: This procedure will establish a standard for employees of the West Virginia Office of Technology (WVOT) in the creation of strong network, mainframe, and email passwords, the protection of those passwords, and the frequency of change. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1000	<p><u>Policy and Procedure Development</u> Summary: This policy establishes the form and content criteria for the West Virginia Office of Technology (WVOT) regarding information technology (IT) policy and procedure development, maintenance, and distribution to agencies within the State of West Virginia Executive Branch. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; compiled all policy definitions; made all references to timelines one year; Added Authority and Enforcement Sections 3.9 and 3.10; Added list of reasons for policy create, modification, or review in Section 3.6; Added information about compliance regulations in Section 3.4.3.</p>
PR1001	<p><u>Technical Investigations</u> Summary: The purpose of this Procedure is to specify the process for State agencies when requesting an investigation into any State employee's technology-based activity. This procedure should not be construed to convey any expectation of privacy. Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions; minor textual edits.</p>

Doc. #	Policy Information
PO1017	<p><u>Use of Social Media</u></p> <p>Summary: Social media/social networking provides an additional method for communicating with West Virginia State Citizens; State agencies; agencies outside the State; business partners; and current, future, and former employees. It is an optional model for interaction that can assist employees in building stronger, more successful citizen and agency business relationships. This document provides policy for the professional use of internal and external social media (i.e. Facebook, Twitter, YouTube, Flickr, etc.) at State of West Virginia Executive agencies.</p> <p>Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1019	<p><u>Wireless Access Point</u></p> <p>Summary: This document prescribes how wireless technologies will be deployed, administered, and supported to assure that State of West Virginia employees, guests, and contractors have access to a reliable, robust, and integrated wireless network, and to increase the security of the wireless network to the fullest extent possible.</p> <p>Edits: Added Change Log History; Added sections 7.1.1.1, 7.1.1.2, and 7.1.1.4: “Each agency has different needs and requirements for public internet access. Agencies are encouraged to contact their WVOT Customer Relationship Manager to review available options.”; “Public access points should NOT connect to the WVOT internal use network.” “Agencies should acquire 3rd party solutions, where feasible, to keep public and private networks physically separated and distinct.”; “At a minimum, all public traffic must be segmented from the State traffic on the internal network if a 3rd party alternative is not available.” Modified Section 4.4.4 – “WPA (minimum) encryption.”</p>
PO1029	<p><u>WVOT Computrace Policy</u></p> <p>Summary: This procedure sets standards for the use of Computrace software by WVOT personnel. Computrace is software created by the company Absolute. This software allows WVOT and its customer agencies theft recovery, data protection and secure asset tracking services.</p> <p>Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>
PO1020	<p><u>WVOT Data Center Security Policy</u></p> <p>Summary: This policy establishes the form and content criteria for the West Virginia Office of Technology (WVOT) regarding information technology (IT) policy and procedure development, maintenance, and distribution to agencies within the State of West Virginia Executive Branch.</p> <p>Edits: New!</p>
PO1026	<p><u>WVOT Monitoring Policy</u></p> <p>Summary: The purpose of this document is to outline the West Virginia Office of Technology (WVOT) policy regarding the monitoring and logging of network traffic that traverses the WVOT Backbone. The goal of monitoring is to maintain the integrity and security of the State’s network infrastructure and information assets. Any inspection of electronic data packets, and any action performed following such inspection, will be governed by all applicable federal and state statutes and by WVOT policies and procedures.</p> <p>Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.</p>

Doc. # Policy Information

PR1009

WVOT Vulnerability Scanning Procedure

Summary: This procedure documents the WVOT methodology for performing and managing security assessments through the execution of vulnerability scanning. Vulnerability scanning is an important and necessary component of any computer security plan as it provides feedback on the effectiveness of security procedures and can alert system administrators to potentially serious problems

Edits: Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions.