1.0 PURPOSE

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.

2.0 SCOPE

This policy applies to all employees engaged in developing technology policies or procedures, unless classified as "exempt" in West Virginia Code Section 5A-6-8, "Exemptions." The State's users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Instant Messaging services.

3.0 POLICY

3.1 Every employee is responsible for abiding by all State IT policies and relevant procedures.

3.2 State employees may view all policies by accessing the WVOT Internet policy page at: go.wv.gov/wvotpolicies

3.3 Agency Responsibilities

3.3.1 Agencies may establish more stringent IT policies; however, duplication of content should be avoided.

3.3.2 Each agency developing a security policy supplement **must** submit it to the WVOT for review.

3.3.3 Agency management is responsible for communicating IT policies and procedures to all current State employees.

3.3.4 Each agency will designate an individual who will be responsible for reviewing all policies and procedures, if applicable, with all newly transferred and hired employees.

3.4 WVOT Responsibilities

3.4.1 The WVOT Policy Unit within the Cyber Security Office (CSO) is responsible for developing and maintaining effective IT and Information Security policy and procedure. This Unit works closely with interested and affected individuals, technical editors, and subject matter experts, as needed.

3.4.2 The WVOT is responsible for establishing and coordinating IT policies and procedures. Final authority for WVOT policies falls to the CTO.

3.4.3 Both State IT policies and procedures are defined by a set of criteria in order to provide consistency and to comply with the multiple local, state, and federal regulations that need followed for compliance.

3.5 Review and Modification

3.5.1 The WVOT will designate an individual(s) to review and amend (as needed) IT policies and procedures annually.

3.5.2 Substantive changes to policy or procedure may only be made with CTO approval.

3.5.3 When revisions to a policy or procedure are necessary, the CTO will determine whether the changes will require a global notification.

3.5.4 Approved policies and procedures remain in effect and are only replaced at the release of a new or modified document.

3.5.5 Any modified or temporary policy or procedure that materially affects the usage rights or responsibilities of employees will be communicated to agencies by a global e-mail message alert or ISA contacts.

3.6 Issues that may trigger policy creation, review, or modification include:

3.6.1 Recognition of a need (for example, legislative requirement, audit outcomes);

3.6.2 Changes in strategic direction and plans;

3.6.3 The Policy and Procedure Development and Review Schedule or an accumulation of issues logged with the Manager;

3.6.4 Identification of content gaps or overlaps across or between policies; or,

3.6.5 The review date of the policy.

3.7 Emergency Temporary Policies

3.7.1 Under certain conditions, the CTO may need to set emergency temporary policies, which will take effect immediately.

3.7.2 The emergency temporary policy will remain in effect for 180 calendar days from the date signed by the CTO. The date may be extended as necessary.

3.8 Maintaining Policies and Procedures

3.8.1 Any State employee may either request that a new IT policy or procedure be written, or propose that revisions to an existing document be made.

3.8.2 Policies and procedures related to information and data system security are reviewed annually, updated as needed, and approved by the relevant department, CISO, and then by the CTO.

3.8.3 The WVOT is responsible for posting and maintaining all IT policies on the State's policy web page: (www.technology.wv.gov). Procedures will be posted to the Intranet only.

3.8.4 To ensure consistency, the WVOT has created a standard format for both policies and procedures to facilitate the adoption of clear, concise documents at all levels of State agencies.

3.9 Authority

3.9.1 Under the provisions of West Virginia Code §5A-6-4a *et seq*., the Chief Technology Officer (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats.

3.9.2 The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

3.9.3 This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

3.9.4 To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy.

3.9.5 In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

3.10 Enforcement Powers

3.10.1 Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal.

3.10.2 Disciplinary action will be administered by the employing agency and may be based upon recommendations of the WVOT and the West Virginia Division of Personnel.

3.10.3 Violations of this policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

3.10.4 The State may also be required by law to report certain illegal activities to the proper law enforcement agencies.

4.0 RELEVANT MATERIALS/DOCUMENTS

This policy is consistent with the following federal and state authorities:

- 45 Code of Federal Regulations (CFR) §§ 164.308-316
- Freedom of Information Act
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Privacy Rule
- NIST SP 800-14 and NIST SP 800-53
- State Health Privacy Laws
- WV Code § 5A-6-4a
- WV Executive Order No. 7-03
- WVOT Policies Issued by the Chief Technology Officer (CTO), www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

5.0 ENFORCEMENT & AUTHORITY

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 the WVOT and the **West Virginia Division of Personnel**. Please review Sections 3.9 and 3.10 of this policy to review additional provisions concerning enforcement and policy authority.

6.0 FULL POLICY DEFINITIONS

6.1 Access Controls – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

6.2 Access– The ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.

6.3 Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within Executive Branch agencies.

6.4 Anti-Virus Software – Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.

6.5 Anti-Virus Team Lead – The functional supervisor of the Anti-Virus Team.

6.6 Authentication – The process of verifying the identity of a user.

6.7 Back-up Files – Electronic files created to restore system files that have become inaccessible on a system.

6.8 Business Records - A document that is used to store information from business operations. Types of operations having business records include meetings and contracts, as well as transactions such as purchases, bills of lading and invoices. Business records can be stored as reference material and reviewed later

6.9 Certification - Certification is an evaluation process assessing non-technical and technical security management, operations, and technical controls, policy, and requirements. Together with a risk analysis and a vulnerability assessment, certification produces documents that support management decisions.

6.10 Certification and Accreditation (CaA) – Validation process that insures that the West Virginia Office of Technology validates the security readiness for devices, systems, software, and other technology prior to deployment of technology into a production status. This validation includes appropriate reviews and/or testing of configurations, hardening, functionality and compliance with specifications, regulations, standards and objectives the generated the deployment activities.

6.11 Change Requesters -- This may be anyone who requests a change to an information system. For example, the Change Requester for an application program modification may be an application analyst. The Change Requester for a change to the computer room will be the Director of Computer Operations or the Director's designee.

6.12 Chief Information Security Officer (CISO) – Person designated by the CTO to oversee information security practices and initiatives for the Executive Branch of WV State government, excluding the constitutional officers.

6.13 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

6.14 Compromise - a vulnerability that has been found and exploited by an unauthorized user.

6.15 Computer Virus – A piece of potentially malicious software that is designed to cause some unexpected or undesirable event, and is generally introduced to a system without the knowledge or consent of the user.

6.16 Confidential Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

6.17 Configuration Management Team – A team within WVOT responsible for making changes to the computer and network architecture.

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

6.19 Criticality - Being of the highest importance. The level at which it data must be protected from non-recovery.

6.20 Custodian of Information – The person or unit assigned to supply services associated with the data.

6.21 Data owner – The entity having primary responsibility for the creation and maintenance of the data content.

6.22 Encryption -- An effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

6.23 E-mail – The transmission of messages over communications networks.

6.24 E-mail System – A service that sends messages on devices via local or global networks. E-mail systems provide for storage, and later retrieval of messages and attachments, as well as real-time communication.

6.25 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.

6.26 Enterprise Change Management Committee - Consists of directors and managers from multiple areas of WVOT, who make appropriate determinations

6.27 Freedom of Information Act (FOIA) - A federal law that mandates that all the records created and kept by federal agencies in the Executive Branch of government must be open for public inspection and copying. The only exceptions are those records that fall into one of nine exempted categories listed in the statute.

6.28 Health Insurance Portability and Accountability Act (HIPAA) – A US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers. Developed by the Department of Health and Human Services, these standards provide patients with access to their medical records and more control over how their personal health information is used and disclosed.

6.29 Individual Contracts – Contracts with individuals for the purpose of providing a specific product or service to the State.

6.30 Information Assets – Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

6.31 Information Resources – Any information in electronic, audio-visual or physical form, or any hardware or software that makes possible the storage and use of information.

6.32 Information Security – Those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

6.33 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency's compliance with State information security policies and procedures. The ISA is the agency's internal and external point of contact for all information security matters.

6.34 Information Security Incident – An event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

6.35 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.

6.36 Information Technology (IT) – The technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.

6.37 Informational E-mail Messages – Messages that are generally of temporary value, consisting of content created primarily for the informal communication of information.

6.38 Instant Messaging (IM) – The technology that allows a user to send electronic messages to one or more persons with minimal delay between the sending and receipt of a message. Like conversation, IM is a simultaneous give-and-take, but it occurs in written form. In contrast to e-mail, which remains unread in a recipient's in-box until opened; instant messaging notifies users when other users are online and able to accept messages.

6.39 Internet - A publicly accessible system of networks that connects computers around the world via the TCP/IP protocol.

6.40 IT Policy – Written statements defining requirements and compliance mandates in the conduct of employees of the State of West Virginia. Only the CTO may issue policy statements relating to IT.

6.41 ITECH Contractors – A list of pre-approved vendors used by the State, who compete for individual staffing needs based upon criteria developed by the agency and the WVOT.

6.42 Just Cause – a legal and legitimate reason.

6.43 Mass Mailings – Information shared with a group of people who all need to know the same material, (ex., committee members, individual units within Bureaus, etc.).

6.44 Medium – Any repository, including paper, used to record, maintain, or install information or data.

6.45 Network Backbone – The physical and electronic network infrastructure, currently under the operational administration of the WVOT.

6.46 Network Violation Report (NVR) – A summary of 24 hours of activity supporting the contention that a serious policy violation has occurred.

6.47 Cyber Security Office (CSO)) - The functional unit charged with the responsibility to undertake and sustain initiatives to promote, enhance, monitor, and govern actions, standards, and activities necessary to safeguard data and information systems within the Executive Branch of WV, as provided in West Virginia Code §5A-6-4a and the Governor's Executive Order No. 6-06.

6.48 Open Network – An area that allows persons using laptop computers equipped with wireless network cards to connect to the WVOT network, via a VPN.

6.49 Owner of Information – The person(s) ultimately responsible for an application and its data viability.

6.50 Password – A string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

6.51 Peer-to-Peer Software (P2P) – A type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives.

6.52 Personally Identifiable Information (PII) –Includes all protected and non-protected information that identifies, or can be used to identify, locate, or contact an individual.

6.53 Privacy Officer - The official responsible for facilitating the Executive Branch's integration of privacy principles, legal requirements, and privacy standards into department policies, procedures, and practices.

6.54 Procedure – A set of instructions or process steps prescribed in sufficient detail in order to understand how to meet a policy requirement. Procedures should document roles, methods, options, and examples necessary for a reader to understand how to comply with a policy.

6.55 Retention Interval – Specifies how long the e-mail (sent or received) needs to be kept to satisfy administrative, legal, fiscal, and historical requirements.

6.56 Risk – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

6.57 Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

6.58 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.).

6.59 Secured ("Closed") – An area that allows State personnel using laptop computers equipped with wireless network cards to connect to the WVOT network directly. A network reserved for State of West Virginia employees and agencies. These wireless networks require password

6.60 Security Contact – These individuals include the ISA or the ISL.

6.61 Sensitivity - The level at which data must be protected from disclosure.

6.62 Social Media – Social media includes web- and mobile-based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals. Examples are Facebook, MySpace, Twitter, YouTube, etc.

6.63 Social Networking – In the online world social networking is the term used to describe the way that users build online networks of contacts and interact with these personal or business friends in a secure environment. Some of the most popular social networking sites include Facebook and Twitter.

6.64 SSID – A Service Set Identifier is a name that identifies a wireless network. All devices on a specific wireless network must know its SSID.

6.65 State Records – Documentary materials or information, regardless of physical media or characteristics, made or received by an office in connection with the transaction of official business, and preserved by that office as evidence of the State's functions, policies, decisions, procedures, operations, or other activities of that office, or because of the value of the data in the record. These messages can set policy, establish guidelines or procedures, capture a dialogue, certify a transaction, or become a receipt.

6.66 State-Use Contracts – Contracts with specific outside companies to provide custodial services to State agencies.

6.67 System – A combination of hardware, software, and procedures necessary to support particular data. A server may have multiple systems and a system may require multiple servers.

6.68 System Owner - The entity who has overall responsibility for a computer application. This person might be required to approve design changes, updates, new reports, system access, or any other action pertaining to the disposition of the application, or data associated with that application. This person would be a subject matter expert (SME) on the system's purpose, hardware requirements, communications requirements, funding requirements, user criteria, etc.

6.69 Temporary Services Contracts – Contracts with temporary service agencies, which offer clerical or secretarial assistance.

6.70 Terms of Service (TOS) – Rules by which one must agree to abide in order to use a service. It is generally assumed such terms are legally binding.

6.71 Threat – Includes any person, condition, or circumstance that endangers the security of information or information systems in the context of information security.

6.72 USB Drive – A plug-and-play portable storage device that uses flash memory and is lightweight enough to attach to a key chain. A USB drive can be used in place of a floppy disk, Zip drive disk, or CD.

6.73 User – A person authorized to access an information resource.

6.74 User ID – A unique "name" by which each user is identified to a computer system.

6.75 Web – World Wide Web means the complete set of documents residing on all Internet servers that use the HTTP protocol, accessible to users via a simple point-and-click system. Sometimes the WEB and "Internet" are used as if they mean the same thing, however, the Internet is actually the network infrastructure that supports the WEB.

6.76 West Virginia Division of Personnel – A 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.

6.77 West Virginia Office of Technology (WVOT) - The division of the Department of Administration established by WV Code § 5A-6-4a*, et. seq.,* which is led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.

6.78 Wireless Access Point - Any piece of equipment that allows wireless communication using transmitters and receivers to enable communications.

6.79 Workstation – A personal computer; also called a PC.

6.80 WVOT Policy Unit - The Unit responsible for developing and maintaining IT and/or Information Security policy and procedure.

7.0 CHANGE LOG

- July 1, 2015 –
  - 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.
- 9/1/2016
  - Policy Reviewed, no edits made.
- 10/20/2017
  - Policy Reviewed, no edits made.