1.0 PURPOSE

This policy, issued by the West Virginia Office of Technology (WVOT) establishes objectives and responsibilities for all West Virginia state government agencies, employees, vendors, and business associates, specifically the Executive, regarding information security and the protection of information resources. The intent of this policy is to explain the range of acceptable and unacceptable uses of State-provided information technology (IT) resources and is not necessarily all-inclusive. IT resources may include anything with a processor, communications capability, or data storage. (See Appendix A, "Technology Usage Practices" for a list of examples.)

2.0 SCOPE

This document applies to all employees with access to information and the systems that store, access, or process that information. Questions about specific security-related uses which are not detailed in this policy should be directed to a supervisor or manager.

3.0 POLICY

3.1 All IT assets, including hardware, software, and data, are owned by the State, unless accepted by contractual agreement.

3.2 Users are required to comply with legal protection granted to programs and data by copyright and license. No unauthorized software will be installed on State systems. The WVOT or its equivalent will authorize all software installation.

3.3 Users will utilize, maintain, disclose, and dispose of all information resources, regardless of medium, according to law, regulation, and/or policy.

3.4 **Employees must have no expectation of privacy while using State-provided information resources (e.g. cell phones, Internet, etc.).**

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

3.6 Agencies are required to have employees sign a policy Statement of Acknowledgement, which will recognize that the employee has read the document and will periodically review the WVOT policy and procedure for updates. Employees may be denied the use of information resources by refusing to sign.

3.7 All employees must adhere to rules regarding unacceptable uses of IT resources. (For a detailed list of unacceptable uses, see appendix A, "Technology Usage Practices")

3.7.1 Employees must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (e.g. downloading MP3 files and/or broadcast audio or video files).

3.7.2 Employees must not intentionally introduce a virus into a State-provided computer, or withhold information necessary for effective virus control procedures.

3.7.3 Employees must not send or share confidential information for unauthorized purposes.

3.7.4 Employees must not attach or use devices on the State network that are not owned by the State or authorized by the WVOT.

3.7.5 Employees must not redirect confidential or privileged State data to a non-State owned computing device or PDA without proper authorization.

3.7.6 Employees must not use unauthorized peer-to-peer networking or peer-to-peer file sharing.

3.7.7 Employees must NEVER execute programs or open e-mail attachments that: (1) have not been requested; or (2) come from an unknown source. If in doubt and lacking assurance from the sender, employees should contact the WVOT Service Desk for assistance.

3.7.8 Employees must never attempt to disable, defeat, or circumvent any security firewalls, proxies, web filtering programs, or other security controls.

3.7.9 Employees must not use IT resources to promote harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability.

3.8 The WVOT, working with designated individuals, will develop procedures to protect information resources from accidental, unauthorized, or malicious access, disclosure, modification, or destruction.

3.9 Users must report any observation of attempted security or privacy violations to incident@wv.gov.

3.9.1 A Security Incident is any event that involves misuse of computing resources or is disruptive to normal system or data processing operations. Examples include, but are not limited to the following:

- Lost or stolen computers or other portable devices;
- Lost or stolen media that contains sensitive data;

- Rampant computer virus infections within the State network;
- Loss of system or network functionality;
- A disaster scenario or act of terrorism;
- A prolonged power outage;
- A compromised (hacked) computer or server;
- A defaced Web page; and
- An information security policy violation.

3.10 Users should immediately report all information security incidents to incident@wv.gov. Users must provide the following information, to the extent possible:

3.10.1 Point of contact (name, phone, e-mail);

3.10.2 Characteristics of incident;

3.10.3 Date and time incident was detected;

3.10.4 Extent of impact;

3.10.5 Nature of incident, if known (ex: unauthorized access, system breach or malfunction, data loss or exposure, defacement, other); and

3.10.6 Any actions taken in response to the incident.

3.11 Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI), or other sensitive data (i.e. credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or disassociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.

3.12 Employees must immediately contact incident@wv.gov upon receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified) or becoming aware of any inappropriate use of State-provided IT resource.

3.13 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.

3.14 Access controls must be consistent with all state and federal laws and statutes, and will be implemented in accordance with this policy.

3.15 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.

3.15.1 All passwords are confidential and **must not** be shared under any circumstances.

3.15.2 Employees are expected to use strong passwords, which must conform to established standards and will be changed at intervals designated by the CTO.

3.16 All access to computing resources will be granted on a need-to-use basis.

3.17 Individual users will be assigned unique userids.

3.18 Each employee must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.

3.19 The WVOT will provision network user accounts by adding, modifying, and deleting user access for customer agencies. Each agency will appoint a designated approval authority, who will authorize all access modifications for that agency.

3.19.1 When an employee is terminated, the agency's designated approval authority must contact WVOT immediately to disable all access, unless otherwise approved in writing by appropriate management.

3.19.2 When an employee transfers, WVOT will modify all access to accommodate new user roles and responsibilities according to instructions from the agency's designated approval authority.

3.20 All Executive Branch employees will be required to complete mandatory online information security awareness or refresher training annually. New employees will be required to complete mandatory online training within the first week of employment as part of job orientation.

3.21 The authorized head of each agency (agency head) must assure that all employees sign a confidentiality agreement upon hire and annually thereafter. This confirms that the employee has read, fully comprehends, and will abide by State policies and procedures regarding privacy and information security.

3.22 The agency head must assure that all employees, and others who access computer systems, will receive sufficient training in policies and procedures, security requirements, correct use of information resources, and other administrative controls.

3.23 The agency head must assure that all employees receive an appropriate background check (where applicable) consistent with legislative rule and West Virginia Division of Personnel policy.

3.24 Data/Information Assets

3.24.1 Information resources are designated for authorized purposes. The State has a right and a duty to review questionable employee activity. Only minimal personal use of State-provided IT resources is permitted (e.g. 10-15 minutes during break and/or lunch periods). This must not include any unauthorized uses (see appendix A) and must not interfere with the legitimate business of the State.

3.24.2 All information assets must be accounted for and have an assigned owner. Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.

3.24.3 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information, according to a classification scheme common to all State agencies. Classification should consider legal protections, privacy, sensitivity, and criticality to the functions of the business. (For more information see WVOT-PO1006 – "Data Classification.")

3.24.4 The owner or custodian will determine and document the data classification, and the agency Information Security Administrator (ISA) will ensure the protective guidelines that apply for each level of information. They include, but may not be limited to the following:

- Access
- Use Within <Agency>
- Disclosure Outside <Agency>
- Electronic Distribution
- Disposal/Destruction

3.24.5 If at any time equipment or media changes ownership or is ready for disposal, the user must alert the responsible technical staff to the potential presence of any confidential and/or sensitive data on said equipment or media.

3.25 Physical and Environmental Security

3.25.1 Information resource facilities will be physically secured by measures appropriate to their critical importance.

3.25.2 Security vulnerabilities will be determined, and controls will be established, to detect and respond to threats to facilities and physical resources.

3.25.3 Employees must guard against access to files and take precautions to protect IT devices when away from the workstation. This includes but may not be limited to the following:

- Logging off computer;
- Locking computer; and/or
- Locking file cabinets and drawers.

3.25.4 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

3.25.5 Equipment will be secured and protected from physical and environmental damage.

3.25.6 Equipment used outside State premises will be given an equal or greater degree of security protection as that of on-site information resource equipment.

3.26 Information Security Administrators

3.26.1 The departmental head must assign the role of Information Security Administrator (ISA). The ISA must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy and the Governor's Executive Information Security Team (GEIST) charter. If necessary, the ISA may delegate duties to one or more individuals (ex: ISL's) whose main function will be to assist in the protection of information resources within their agency.

3.26.2 The ISA will ensure that a risk management program will be implemented and documented, and that a risk analysis will be conducted periodically.

3.26.3 The ISA will oversee and ensure that cost effective contingency response and recovery plans will be maintained, providing for prompt and effective restoration of critical business functions in the event of any disruptive incident.

3.26.3.1 Procedures, guidelines, and mechanisms utilized during an information_security incident, along with the roles and responsibilities of the incident management teams, must be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.

3.26.3.2 Testing will be performed at intervals designated within CTO standards.

4.0 RELEVANT DOCUMENTS/MATERIAL

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 the **WVOT Policy and Procedure Policy #1000** to review additional provisions concerning enforcement and policy authority.

6.0 DEFINITIONS

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

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

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

6.4 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.

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

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

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

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

6.9 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.

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

6.11 Information Resources – All information assets, in all known formats.

6.12 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.

6.13 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.

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

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

6.16 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.

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

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

6.19 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.

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

6.21 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.

6.22 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.

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

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

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

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

6.27 User id – A unique “name” by which each user is identified to a computer system.

6.28 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.

6.29 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.

7.0 Change Log History

- January 28, 2015 – 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….”

Acceptable/Unacceptable Use of State-Provided Technology:

The information contained within this Appendix applies to the State of West Virginia Information Security policy.

Relevant Technologies Include, but may not be limited to the following:

a. Personal computers
b. Personal Digital Assistants (PDA)
c. Fax or copy machines with memory or hard drives
d. Internet or Intranet
e. E-mail and Enterprise Instant Messaging (EIM)
f. Voice Mail
g. Cell phones (including camera phones and smart phones with data communications and databases)
h. Pagers
i. Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives)
j. Servers
k. Printers

Unacceptable uses include, but are not limited to the following:

a. Any use which violates local, state, or federal laws;
b. Any use for commercial purposes, product advertisements, or “for-profit” personal activity;
c. Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
d. Any use for promotion of political or religious positions or causes;
e. Any use in relation to copyright infringement.
f. Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;
g. Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
h. Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
i. Any use for dispersing data to customers or clients without authorization;
j. Any use in relation to placing wagers or bets;
k. Any use that could be reasonably considered as disruptive to another’s work;

1. Employees will not waste IT resources by intentionally doing one or more of the following:

    a. Placing a program in an endless loop;
    b. Printing unnecessary amounts of paper;
    c. Disrupting the use or performance of State-provided IT resources or any other computer system or network; or
    d. Storing unauthorized information or software on State-provided IT resources.

2. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:

    a. Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;
    b. Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
    c. Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
    d. Misrepresenting oneself or the State of West Virginia;
    e. Making statements about warranty, express or implied, unless it is a part of normal job duties;
    f. Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the WVOT; or
    g. Transmitting through the Internet confidential data to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the WVOT

3. Employees will not commit security violations related to e-mail activity. This includes doing one or more of the following:

    a. Sending unsolicited commercial e-mail messages, including the distribution of "junk mail" or other advertising material to individuals who did not specifically request such material;
    b. Unauthorized use for forging of e-mail header information;
    c. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies;
    d. Posting messages to large numbers of users (over 50) without authorization; or
    e. Posting from an agency e-mail address to newsgroups, blogs, or other locations without a disclaimer stating that the opinions expressed are strictly their own and not those of the State or the agency, unless posting is in the fulfillment of business duties.

Employee Responsibilities

Employees should conduct themselves as representatives of the State, and are responsible for becoming familiar with and abiding by all information security policies and guidelines.

1. Employees will only access files, data, and protected records if:

    a. The employee owns the information;
    b. The employee is authorized to receive the information; or
    c. The information is publicly available.

2. Employees are prohibited from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, bandwidth, disk space, printer paper, or other IT resources.

3. Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.

4. Employees must adhere to copyright law regarding the use of software, print or electronic information, and attributions of authorship. In certain instances, legal counsel can determine permissible uses.

Appendix B: Policy Understanding and Acknowledgment

Policy: Information Security

State of West Virginia Office of Technology

INFORMATION TECHNOLOGY POLICIES ACKNOWLEDGMENT

From West Virginia Office of Technology
Office of Information Security and Controls

I have read, understand, and agree to abide by the following West Virginia Office of Technology Information Technology Policies:

- Information Security Policy (WVOT-PO1001)
- Acceptable/Unacceptable Use of State-Provided Technology (WVOT-PO1001, Appendix A)

I understand and agree that if I violate any of the provisions of any of these policies I may be subject to disciplinary action up to and including termination.

Signature _____ Date _____

Printed Name _____

Signature Supervisor _____ Date _____

Printed Name of Supervisor _____