1.0 PURPOSE

The State must diligently protect its information technology assets, State employees, environment, and information system integrity from the risks associated with:

- accessing websites that create a hostile work environment, contain sexually explicit material or otherwise violate the Department of Personnel Harassment Policy,
- downloading or installing unauthorized software, illegal software, or copyrighted material on State computing devices, or
- visiting Internet sites that may be dispensing malware to the visitor.

To accomplish this, tools are used to monitor computer, Internet, and network activity and traffic. When non-standard software and data flows are detected, their location or destination is pinpointed, and the user responsible is identified.

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.

2.0 SCOPE

This policy applies to all Departments (including agencies, boards, and commissions) within the West Virginia State Government which uses State equipment or networks.

3.0 Policy

3.1 When the Security Operations Center (SOC) detects and confirms user violations, a summary Network Violation Report (NVR) and full evidence disk will be created and conveyed to the agency Point of Contact (POC).

3.2 Examples of network violations include the following:

3.2.1 Accessing prohibited Web sites, which include:

3.2.1.1 Pornography;

3.2.1.2 Gambling;

3.2.1.3 Violence;

3.2.1.4 Bias or hate speech;

3.2.1.5 Illegal use of weapons;

3.2.1.6 any other category as decided by the Agency; or,

3.2.1.7 the Department of Personnel Harassment Policies.

3.2.2 Installing peer-to-peer (P2P) software to download material (games, software, music, videos, etc.), which could create an unmanaged entry point into the network, allowing public access to a portion or all of the computer hard drive, and potentially access beyond these boundaries.

3.2.2.1 Following the detection of unauthorized software or data within the Enterprise, and the identification of the responsible user, specific actions will be taken to engage agency officials, initially via the POC or designee, to remediate the violation. This will include removing any unauthorized software or data from the affected computer(s), and informing agency management of the user's violation, in order to prevent a recurrence of the offense.

3.2.3 Willful introduction of malicious content (viruses, Trojans, etc.) into the State computing environment by opening malicious e-mail attachments, visiting malicious web sites, and inserting USB drives or other personal devices that have been loaded with malicious executable code, etc.

3.2.4 Repeated violations of WVOT policies against streaming non-business related or unauthorized audio/video content, causing overconsumption of bandwidth which can adversely impact productivity of other users.

3.2.5 Willful and reckless neglect of IT information security policies and procedures.

3.3 The WVOT reserves the right to protect the network from ongoing or severe employee policy violations by disabling internet or network access.

3.3.1 WVOT will **not** be responsible for any employee disciplinary actions.

3.3.2 This policy shall **NOT** be construed to limit an executive agency's authority to discipline an employee who violates state or federal laws or state policy.

3.4 Escalation of Offenses

3.4.1 After the first notification of an NVR, the Agency has 5 business days, or earlier, to notify Enterprise Security of any action being taken.

3.4.2 After 5 days, monitoring will resume on the original NVR.

3.4.3 If a violation occurs again, a second NVR and evidence disk will be sent to the Agency POC.

3.4.3.1 If the Agency chooses not to suspend the user's internet or network access, a Risk Acceptance Memorandum will need to be signed by the Cabinet Secretary, accepting the risk that the user's Internet access is subject to revocation if network violation activity is detected again.

3.4.3.2 After 5 business days, monitoring will resume.

3.4.4 If a third violation triggers an NVR, then Internet access will immediately be suspended and Agency leaders and WVOT personnel will meet to discuss actions to mitigate ongoing risk.

3.4.5 The WVOT will schedule and complete software and/or file removal after each NVR occurrence, (P2P or other unapproved software, e.g. Limewire, Kazaa, Bit Torrent, Napster, copyrighted material, inappropriate content, etc.), when applicable, as soon as possible.

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

6.0 POLICY-SPECIFIC DEFINITIONS

6.1 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.

6.2 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.

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

6.4 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.

6.5 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.

7.0 CHANGE LOG

- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions; Removed acknowledgment form (consolidated into training);
- 9/1/2016 – Policy Reviewed. No edits made.
- 10/20/2017- Policy Reviewed. No edits made.