1.0 PURPOSE

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.

2.0 SCOPE

This policy applies to all users, agencies, departments and offices of information technology resources operating on the State's Network.

3.0 POLICY

3.1 Backbone network traffic will be monitored for the improper release of confidential information, intruder detection, and other security or policy violations.

3.2 Personnel authorized to analyze the network backbone will not disclose any information reviewed in the process without approval of the Chief Technology Officer (CTO) or Chief Information Security Officer (CISO), and the appropriate agency authority, when appropriate.

3.3 Only the Security Operations Center (SOC) and Networking teams in the WVOT are authorized to routinely monitor traffic. Authorization for ad hoc monitoring may be granted to others *in writing* by the CTO or CISO.

3.4 Authorized staff shall use network monitoring devices only to detect:

3.4.1 known patterns of attack or compromise;

3.4.2 the improper release of data;

3.4.3 or to troubleshoot and analyze network-based problems.

3.5 The scope of all monitoring shall be as narrow as possible.

3.6 Monitoring data stores and logs will not be accessible from the public Internet. All personnel will show due care in to data in compliance with the WVOT Data Classification Policy's requirements for protection, handling, and storage.

3.7 All requests for monitoring assistance from agencies shall be coordinated through the Office of Information Security Controls and Compliance.

3.8 Exceptions to monitoring protocols set forth in this procedure may only be requested by Cabinet Secretaries or Constitutional Officers.

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 DEFINITIONS

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

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

6.3 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.

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

6.5 SOC – Security Operations Center. Monitors the health of the Network Backbone.

6.6 Packet – Electronic unit of data that is routed between an origin and a destination on a network.

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
- 9/1/2016 – Policy Reviewed. No edits made.
- 10/20/2017 – Policy reviewed. No edits made.