1.0 PURPOSE

This policy establishes and communicates the acceptable use of, access to, and disclosure of the State-provided e-mail system. This document is not all-inclusive and management has the authority and discretion to appropriately address any unacceptable behavior and/or practice not specifically mentioned herein.

2.0 SCOPE

This policy applies to all employees within the Executive Branch using the State-provided Email system, 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 Email services.

3.0 POLICY

3.1 All State employees covered under this policy are expected to use the State-provided, centralized e-mail system for official communications. Any deviation must be approved by the WVOT.

3.2 All State content sent and/or received by email is owned by the State and may be considered official State records.

3.3 Use of personal e-mail or other email services (e.g. Gmail) to conduct State business is strictly prohibited.

3.4 State-provided e-mail is not to be used for the creation or distribution of any offensive or disruptive messages (see *Appendix A* of WVOT-PO1001 – *Information Security Policy*). Executive Branch employees who receive any e-mail containing this content should report it to incident@wv.gov immediately.

3.5 Agency management is responsible for managing the e-mail activities of employees in State agencies.

3.6 **Employees have no expectation of privacy in anything they create, store, send, or receive on the State-provided email.**

3.6.1 Password protecting an e-mail account does not confer a special status or access limitation/restriction on e-mail or any records with respect to privacy and applicability of laws, policies, and practices.

3.6.2 The State reserves the right to monitor and/or keep a record of all e-mail communications without prior notice or consent.

3.6.2.1 The WVOT does not routinely monitor, or authorize e-mail monitoring, but may, with just cause, access and/or disclose the e-mail or files of an employee, provided it follows appropriate procedures and authorization mechanisms designed to assure compliance with State policies and applicable law.

3.6.3 The contents of e-mail messages properly obtained for discovery or management purposes may be disclosed without the permission of the authorized user who created the message.

3.6.3.1 E-mail system administrators will retain a limited history of back-up files for disaster recovery or e-Discovery purposes only. These files will not routinely be used to recover individual messages or mailboxes.

3.6.3.2 Copies of e-mail messages held on back-up systems will remain accessible and may be subject to legal discovery and monitoring.

3.6.3.3 Each agency may have specific supplemental retention requirements. The agency head is responsible for training employees with respect to retention criteria applicable to agency data, including the length of time State records warrant retention for administrative, legal, or fiscal purposes after the agency has received the email messages.

3.7 Within the State's e-mail system, all messages, attachments, files, and folders are automatically encrypted.

3.7.1 Messages sent outside of the system are NOT encrypted automatically. If sensitive data is being transmitted outside the State enterprise via email, the State's e-mail encryption tool, or an approved substitute, must be used.

3.7.2 Users must get approval for Encryption Services by their agency management and may contact the WVOT Service Desk for more information.

3.8 Employees must follow any agency- or department-specific guidelines when sending mass mailings or group messages.

3.9 Employees must never open email attachments that have not been requested, or that come from an unknown source.

3.10 Agencies handling Federal Tax Information (FTI), must comply with all *IRS Publication 1075* safeguards, as well as the following State requirements:

3.10.1 Agencies with access to FTI must have a procedure in place that articulates the protocols of using electronic mail for transmitting and receiving files containing FTI.

3.10.2 FTI should not be transmitted or used on an agency's internal e-mail systems, unless absolutely required to complete a business function.

3.10.3 FTI must not be transmitted outside of agency, either in the body of an e-mail or as an attachment. If transmittal of FTI within the agency's internal e-mail system is necessary, the following precautions must be taken to protect FTI:

- Do not send FTI unencrypted in any e-mail messages.
- Any file attachments containing FTI must be encrypted.
- Ensure that all messages sent are to the proper address.
- Where required, provide the password/encryption key in a separate e-mail or other communication.
- Track files containing FTI received by e-mail.

3.11 Each agency is responsible for meeting any regulatory guidelines specific to their individual business units.

4.0 RELEVANT 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
- IRS Publication 1075
- 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 Back-up Files – Electronic files created to restore system files that have become inaccessible on a system.

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

6.3 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.

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

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

6.6 Just Cause – a legal and legitimate reason.

6.7 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.).

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

6.9 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.

7.0 Change Log History

- July 1, 2015 –
  - Added Section 7.0, Change Log History; Reorganized sections; Cleaned up Related Documents/Materials; Made Policy-Specific Definitions