1.0 PURPOSE

The reliability and timely availability of electronic records and system applications is critical to the success of the State of West Virginia (State) operations.

This policy outlines data backup requirements for the West Virginia Office of Technology (WVOT) to ensure availability of critical data and systems within Executive Branch agencies.

2.0 SCOPE

This policy applies to all departments (including agencies, boards, authorities, and commissions) within the Executive Branch of West Virginia State Government, excluding constitutional officers, the West Virginia Board of Education, the West Virginia Department of Education, and the county boards of education that have access to or use State-provided resources.

To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy.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

3.0 POLICY

3.1 Server Backup and Recovery

3.1.1 WVOT utilizes the server data backup system to ensure that agency programs, files, and datasets are properly backed up and retained.

3.1.2 All production environments and data will be backed-up, unless an agency submits a written request to opt out of the production backup process.

3.1.2.1 All server data backup parameters will be specified by agencies and configured by WVOT.

3.1.2.2 Agencies with special backup needs exceeding the requirements of this policy will be identified through technical risk analysis, and will be accommodated on a case-by-case basis.

3.1.2.3 Agencies will be charged for storage at the rate defined in the WVOT rates catalog.

3.1.3 All non-production environments (e.g., development, test, and training) and associated data will not be backed up, unless the agency submits a written request to the WVOT.

3.1.4 Server data backups will be performed based on recovery point objectives. (See Appendix "A" for information on Business Criticality Classes.) If the agency has not defined recovery point objectives, the standard default for data backup will be nightly.

3.1.5 WVOT will monitor backups, address technical issues related to server data backup, and notify agencies of instances when information has not been backed-up according to plan. However, agencies must test to ensure that the backed-up data is accurate and complete.

3.1.6 Agency personnel must contact the WVOT Service Desk either by phone at (304) 558-9966 or by email at servicedesk@wv.gov for all recovery requests.

3.1.7 Data server backup and recovery efforts do not provide disaster recovery services. Additional arrangements must be made for full restoration of operating systems, directory services, etc.

3.1.8 Agencies requesting data restoration must contact the WVOT Service Desk. Requests are tracked through the Problem Management System.

3.2 Mainframe Specific Backup and Recovery

3.2.1 WVOT will perform full volume mainframe backups on a weekly basis. These backups are taken from the main site and stored at an offsite storage location. Rotation cycles for these volumes allow for two (2) full sets, current and previous week's data, to be retained offsite.

3.2.2 Backups will be performed daily for some mainframe datasets deemed by customer/agency to be of a critical nature for system recovery. These backups are taken daily to an offsite storage location and will be retained according to Data Center requirements.

3.2.3 Each agency will perform mainframe data file backups according to its own requirements, as well as determine the data's frequency and retention cycles. All backups will be taken daily to an offsite storage location.

3.3 Monitoring

3.3.1 Mainframe monitoring is configured to automatically notify the agency administrator if a backup has not completed successfully. Failures are escalated and resolved through the WVOT Service Desk.

3.3.2 Server data monitoring is performed on a real-time basis for successful completion. Daily backups and logs will be monitored for success and failure by the WVOT. All failures are reported to the affected agency and WVOT will work with the agency to correct the failure.

3.4 Backup Modifications/Schedule Configuration Changes

3.4.1 Modifications to the supported environment will be determined between the agency and the WVOT prior to implementation. WVOT will perform upgrades to the system, when required, and notify the agency of any changes.

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, part-time, full-time, 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, but not be limited to, 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 Chief Technology Officer (CTO) – The person responsible for the State's information resources.

6.3 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.

6.4 West Virginia Division of Personnel – The 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.

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

6.6 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.

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.