1.0 PURPOSE

This document is intended to provide guidance to agencies and employees about the appropriate use of state-approved cloud service, WVOT's Microsoft One Drive for Business ("One Drive"). This policy contains risk factors all agency leaders and staff must review before using the cloud service. When using One Drive, information is stored remotely on servers owned by Microsoft and located in the continental United States.

2.0 SCOPE

This policy applies to all employees who access the Internet through the computing or networking resources, 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 Internet services.

3.0 POLICY

3.1 To utilize One Drive to receive, transmit, store, or process any data, the agency must ensure a Memorandum of Understanding (MOU) is in place between WVOT and the Agency.

3.2 Agencies may use One Drive when handling Confidential or Public Data.

3.2.1 Refer to Data Classification Policy #1006 for complete definitions of data types.

3.3 Agencies may NOT use One Drive managing Restricted Data unless:

3.3.1 There currently is not a technical solution available or in place.

3.3.2 The Agency's Privacy Officer has completed a Risk Impact Assessment or equivalent review.

3.4 All requests for One Drive use must be authorized by the agency Designated Approval Authority (DAA).

3.4.1 Approval must come from management-level DAAs that are employed with the Agency.

3.5 Agencies must assess, annually, their security in place on all information systems used for receiving, processing, storing and transmitting the sensitive information stored in One Drive.

3.6 Agencies must identify security controls or processes that insure the data is handled correctly and meets any relevant compliance regulations.

3.7 One Drive is not intended for permanent storage of State records.

3.8 One Drive is not intended for group storage. It is based on user accounts.

3.9 Devices accessing One Drive must be securely sanitized and/or destroyed at the end of their life cycle or if the device is lost or stolen.

4.0 RELATED DOCUMENTS/MATERIALS

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 "Cloud services" is a general term used to include a variety of computing and information services and applications run by users across the Internet (in the "Internet cloud") on the service provider's systems, instead of run "locally" on personal computers or campus-based servers. These Internet-based services are sometimes called "software as a service" (SaaS), or "platform as a service" (PaaS), or "hosted" applications, storage or computing.

6.2 Restricted data is the most sensitive data to integrity and confidentiality risks. This data is only made available to authorized users and may be protected by federal and State regulations. Please refer to Data Classification Policy PO1023 for more detailed definitions.

6.3 Confidential: Access to confidential data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their job duties. Please refer to Data Classification Policy PO1006 for more detailed definitions.

6.4 Public Data: This data is made available through open record requests or other formal or legal processes; it includes the majority of the data contained within State government electronic databases. Please refer to Data Classification Policy PO1006 for more detailed definitions.

7.0 Change Log History

7.1 1/25/2016 – Policy Created