1.0 PURPOSE

This policy presents a framework through which all State of West Virginia (State) government agencies, employees, vendors, and business associates, specifically the Executive Branch, should classify data and systems as they relate to (1) data sensitivity; and (2) data and system criticality. (See Attachment A, *Data Sensitivity and System Criticality Grid*)

Consideration must be given to the fact that the same data type may have different sensitivity in different situations (e.g. publishing employee addresses: corrections employees vs. tourism employees).

2.0 SCOPE

This policy applies to all employees within the Executive Branch, 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 Instant Messaging services.

3.0 POLICY

3.1 All State data requires classification, which is mandatory for more sensitive and critical classes of data.

3.2 Each department and/or agency will provide annual certification that the data they collect, maintain, distribute, and ultimately destroy, is categorized in compliance with the data classification scheme prescribed in this policy.

3.3 Data must be properly managed according to its classification.

3.4 Data Classification Levels: Data owned or maintained by agencies will be put into appropriate classification levels, according to its sensitivity and criticality.

3.4.1 Level 1 – **Restricted**

3.4.1.1 **"Restricted"** is the most sensitive data to integrity and confidentiality risks.

3.4.1.2 Access is tightly restricted with the most stringent security controls at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health, or safety repercussions. Individuals must adhere to very strict rules in the usage of this data.

3.4.1.3 Access to **Restricted Data** is protected by federal, State and local regulations, and limited to authenticated and authorized individuals who require access to that information in the course of performing their job duties.

3.4.1.4 These data elements are removed from responses to information requests for reasons of privacy.

3.4.1.5 Security threats to **Restricted Data** include violation of privacy statutes and regulations, as well as unauthorized alteration or destruction. If unauthorized persons accessed this data, it could cause financial loss or allow identity theft. In order to prevent these threats, security controls appropriate to the system containing this data must be in place.

3.4.1.6 Examples of **Restricted Data** may include the following:

- Child and adult protective services client data;
- Attorney-Client communications;
- Computer Vulnerability Reports;
- Contents of State law enforcement investigative records;
- Protected draft communications;
- Social Security numbers;
- Credit card numbers;
- Food assistance programs data;
- Comprehensive law enforcement data;
- Foster care data;
- Health, mental health, acute medical care, and medical data;
- Social Service or Temporary Assistance data;
- HIPAA Security Data (45 CFR Parts 164),
- PCI DSS v2.0,
- FICA
- State Tax Information; and
- Federal Tax Information.

3.4.2 Level 2 – **Sensitive Data**

3.4.2.1 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.

3.4.2.2 Direct access is limited to authenticated and authorized individuals who require access to that information in the course of performing their job duties.

3.4.2.3 Security threats to sensitive data include unauthorized access, alteration, and destruction concerns. Security controls appropriate to the system containing this data must be in place to prevent these threats.

3.4.2.4 Examples of sensitive data may include the following:

- Most data elements in State personnel records;
- Driver history records;
- State/federal contracts data;
- Employment and training program data;
- Permits data; and
- Historical records repository data.

3.4.3 Level 3 - **Public Data**

3.4.3.1 This data is characterized as being open, public data with no distribution limitations and to which anonymous access is allowed.

3.4.3.2 This type of information is: (1) actively made publicly available by State government; (2) published and distributed freely, without restriction; and (3) available in the form of physical documents such as brochures, formal statements, press releases, reports, web pages, and bulletin boards accessible with anonymous access.

3.4.3.3 The greatest security threat to **Public** data is from unauthorized or unintentional alteration, distortion, or destruction. Security controls appropriate to the system containing this data must be in place to maintain its integrity.

3.4.3.4 Examples of **Public** data may include the following:

- Occupational licensing data excluding social security numbers;
- Agency public websites; and
- Statewide policies.

3.5 To utilize a cloud computing services to receive, transmit, store, or process State data, the agency must ensure:

3.5.1 Data is isolated. Software, data, and services that receive, transmit, process, or store data, must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

3.5.2 The service has been vetted and approved by the WVOT Chief Information Technology Officer and Chief Information Security Officer.

3.5.3 Data is encrypted during transit. Restricted and Sensitive data must be encrypted in transit within the cloud environment. All mechanisms used to encrypt the data must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module.

3.5.4 Data is encrypted at rest in the cloud.

3.5.5 Devices accessing the cloud storage can be securely sanitized and/or destroyed at the end of their life cycle or if the device is lost or stolen.

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

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

3.6 All State employees with direct responsibility for State data (i.e. system owners, data owners, managers, and State leadership), must receive training in the data classification scheme appropriate to their role. (For example, State leadership must be trained and fully aware of the classification scheme of their departmental and agency employees who have a role in the maintenance of valid data classification, and of the implications of misclassified or non-classified data.)

3.6.1 Data owners must be trained and aware of the data classification scheme and the physical location of their sensitive and/or restricted data and all secondary copies of that data.

3.6.2 Data owners must provide for the adequate synchronization of primary and secondary copies of this data, and must certify that the controls in place are commensurate with the sensitivity and criticality of the data. This includes access permissions and restrictions controls, as well as recovery strategies for lost or damaged data.

3.7 **Data Criticality:** Data and systems should be put into appropriate classification levels according to their criticality. The levels of criticality and their descriptions are as follows:

3.7.1 **Level A – Extremely Critical** – These data and systems are critical to public health or safety and must be protected by a vital plan allowing the continuation of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business and might require availability within two hours.

3.7.2 **Level B – Critical** – These data and systems are required in order to administer functions within State government that need to be performed. Business continuity planning allows the State to continue operations in these areas within a certain period of time until the data and systems can be restored and might require availability within eight hours.

3.7.3 **Level C - Not critical** – These data and systems are necessary to State government, but short term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of the citizens of West Virginia.

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 Contractor – Anyone who has a contract with the State or one of its entities.

6.2 Criticality - Being of the highest importance. The level at which it data must be protected from non-recovery.

6.3 Data owner – The entity having primary responsibility for the creation and maintenance of the data content.

6.4 Restricted Data – Information that is legally protected (ex: Protected Health Information) or otherwise deemed by a qualified expert to be unsuitable for open access.

6.5 Sensitivity - The level at which data must be protected from disclosure.

6.6 System – A combination of hardware, software, and procedures necessary to support particular data. A server may have multiple systems and a system may require multiple servers.

6.7 System Owner - The entity who has overall responsibility for a computer application. This person might be required to approve design changes, updates, new reports, system access, or any other action pertaining to the disposition of the application, or data associated with that application. This person would be a subject matter expert (SME) on the system's purpose, hardware requirements, communications requirements, funding requirements, user criteria, etc.

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;
- November 6, 2015 –
  - Renamed Classification Categories.
    - "Extremely Sensitive Data" and "Very Sensitive Data" now combine to form the "Restricted" category.
    - "Unrestricted Data" now named "Public Data"
- September 1, 2016
  - Policy reviewed, no edits made.
- October 20, 2017
  - Policy reviewed, no edits made.

	Level A - Extremely Critical Critical to health or safety: These systems must be protected by a vital plan that would allow resumption of operations within a very short timeframe. It also requires the ability to be able to resume business.	**Level B - Critical** Required to perform a critical service of State government: These systems will be required in order to administer critical functions within State government. Business continuity planning allows State government to continue operations in these areas within a certain period of time until the system can be restored.	**Level C - Not Critical** Necessary to State government but short-term interruption of service acceptable. These systems do not play any role in the scheme of health, security, safety of the citizens, etc. They could be easily offset with manual procedures.
Level 1 - **Restricted** Data whose disclosure or corruption could be hazardous to life or health (ex: State law enforcement records). Data only available to internal authorized users. May be protected by federal and state regulations. Intended for use only by those who require information in the course of performing job functions (ex: SSNs, credit card #s, home addresses).	**1A**	**1B**	**1C**
Level 2 - **Sensitive** Public Data with limited availability, but which requires a special application to be completed or special processing to be done prior to access (ex: State personnel records, data elements in motor vehicle records not restricted by privacy regulations, etc.).	**2A**	**2B**	**2C**
Level 3 - **Public** Open public data with no distribution limitations, anonymous access. May be anonymous access via electronic sources.	**3A**	**3B**	**3C**

** Rows Represent Data Sensitivity
** Columns Represent System Criticality