West Virginia Higher Education Policy Commission
West Virginia Community and Technical College System

Data Classification and Protection Policy

1. Purpose

This purpose of this policy is to establish a framework for classifying and protecting the data collected and maintained by the West Virginia Higher Education Policy Commission (Commission) and the West Virginia Community and Technical College System (Council).

This policy is based on the State of West Virginia Office of Technology's Data Classification Policy (WVOT-PO1006), industry standards, best practices recommended by the U.S. Department of Education's Student Privacy Policy Office (SPPO), and adheres to state and federal privacy laws and regulations[1]. This policy is reviewed annually or as circumstances dictate and revised as applicable.

2. Scope

This policy applies to all employees (paid, unpaid, interns, full-time, part-time, technical, and non-technical), vendors, contractors, and all other individuals, collectively referred to as "users", who have access to or use of the data collected and maintained by the Commission and Council. Furthermore, this policy applies to all data collected, maintained, or processed by the Commission and the Council broadly.

3. Authority

The Executive Vice Chancellor of Administration for Commission and Council has appointed a Privacy Officer and named them as the designated authority to establish and maintain a system of data and information security and protection. The Privacy Officer and the Division of Policy and Planning determine the classification of all data and information.

4. Data Classification

All data requires classification to ensure proper handling and protection and all data must be managed according to its classification. Commission and Council data are classified into different levels and each level requires specific security and protection due to the risk impact of the data is mishandled.

[1] *State and Federal privacy laws and regulations include but are not limited to the following: W.V. Code §46A-2A et seq., Family Educational Rights and Privacy Act (FERPA), the Higher Education Act of 1965 as revised in 2008 (HEA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

Level 1 – Restricted

4.1 **Restricted** data is the most sensitive to integrity and confidentiality risks. Data is classified as **Restricted** when unauthorized disclosure could cause a significant level of risk.

4.2 Access to **Restricted** data is protected by federal, state, and local privacy laws and regulations such as FERPA, HEA, and GLBA. Only authorized users who require access to perform their duties will be given access. **Restricted** data must be protected at the highest level possible.

4.3 Unauthorized access has the potential to cause harm to the individual, may violate state or federal privacy regulations, or cause data breaches.

Examples of **Restricted** data may include the following:

- Personally Identifiable Information (PII), which includes any information that by itself or in combination with other information, has the potential to directly determine or find the identity of an individual person and could be harmful to an individual if disclosed; [2]
  - Social security number, state/federal issued personal identification number, or driver's license number;
  - Banking or credit card numbers;
  - Financial information including state and federal tax information;
  - Full name and personal address;
  - Name of student's parent and other family members, or mother's maiden name;
  - Citizenship or immigration status;
  - Health and medical information;
  - Student grades, GPA, ACT or SAT scores;
  - FAFSA or financial aid information;
- Indirect PII is information, when linked or linkable could be used to identify an individual
  - Date or place of birth;
  - Business phone;
  - Race/ethnicity;
- Protected draft communications;
- Computer vulnerability reports;
- Foster care data;
- Health, mental health, and medical data;

Level 2 – Sensitive

4.5 **Sensitive** data is defined as data that if disclosed could result in a moderate level of risk. This includes data that is made available through open record requests or other formal or legal processes.

[2] *See Family Educational Rights and Privacy Act (FERPA) regulations, 34 CFR §99.3, for a complete definition of PII specific to education data and for examples of education data elements that can be considered PII.*

4.6 Direct access is limited to authenticated and authorized individuals who require access to perform their duties.

4.7 Examples of **Sensitive** data may include:

- Most data elements in state personnel records;
- State/federal contracts data;
- Employment and training program data;

Level 3 – Public

4.8 **Public** data is characterized as being open to the public. Information that alone or in combination with other data cannot be used by a reasonable person to identify an individual; furthermore, if disclosed or shared, it would result in little or no risk to the individual or agency.

4.9 This type of information is actively made public, published and distributed without restriction, or available in the form of physical documents, formal statements, press releases, interactive data dashboards, or other ways where the public can access it.

4.10 The greatest threat to **Public** data is from alteration or distortion.

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

- Directory information which includes information that is not generally considered to be harmful to an individual, or an invasion of privacy;
- Enrollment in an institution;
- Official honors and awards received;
- Participation in officially recognized sports;
- Agency public websites;
- Commission and Council policies and procedures;

5. Cloud Services

To utilize a cloud computing service to receive, transmit, store, or process Commission and Council data the following must be ensured.

5.1 A privacy impact assessment must be completed by the Privacy Officer.

5.2 The service must first be vetted by the agency Privacy Officer and/or the Division of Policy and Planning. No data can be transferred, processed, or stored on a cloud service until proper authorization has been given.

5.3 Data must reside in the United States and be isolated so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

5.4 Data must be encrypted during transit. All mechanisms used to encrypt the data must be FIPS 140-2 compliant and operate utilizing the FIPS 140-2 compliant module.

5.5 Data must be encrypted at rest while in the cloud.

5.6 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.

5.7 The cloud service must be compliant with all required state and federal privacy regulations including FERPA, HEA, HIPAA, and GLBA. Other regulations may apply depending on the data that will be involved.

5.8 Proper documentation, contracts, and agreements must be developed and reviewed by the Privacy Officer to ensure compliance with state and federal laws.

5.9 Cloud security must be reviewed for compliance annually.

6. Training and Awareness

All users must be aware and knowledgeable in the Commission and Council's data classification policy.

6.1 All users will be trained and made aware of the data classification levels annually or when changes arise.

7. Data Criticality

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

7.1 **Level A: Extremely Critical** – These data and systems are critical to operations 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.

7.2 **Level B: Critical** – These data and systems are required in order to administer functions within the Commission and Council that need to be performed. Continuity planning allows the Commission and Council 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.

7.3 **Level C: Not Critical** – These data and systems are necessary to the Commission and Council, but short-term interruption or unavailability is acceptable.

8. General Safeguarding Policies

It is important to ensure that **Restricted** and **Sensitive** data is always protected. A privacy incident[3] is defined as an attempted or successful effort to access, acquire, disclose, or use PII or other information without authorization (i.e., any potential or actual unauthorized disclosure). That information may be in various formats, including physical or electronic records, verbal statements, or other reports. These types of incidents can normally be prevented by following

[3] See Commission and Council Incident Response Plan for details on privacy incidents.

privacy procedures and using appropriate controls when sharing or accessing restricted or sensitive information.

There may be times where sharing **Restricted** or **Sensitive** information is necessary. In these instances, you should contact the Privacy Officer or the Division of Policy and Planning who will assist you in determining the most secure method and processes to follow. Policy and Planning has developed several methods that can be used for the secure transfer of **Restricted** or **Sensitive** information.

General Restricted or Sensitive Information Storage and Sharing Rules:

8.1 Never email **Restricted** or **Sensitive** information.

8.2 **Restricted** and **Sensitive** information is to be stored on the secure file folders assigned to each user by the Senior IT Systems Administrator.

8.3 **Restricted** or **Sensitive** information is **never** to be stored on local machines, smart phones, tablets, laptops, USB or flash drives, external hard drives, digital media, or other portable devices without express prior authorization from the Privacy Officer or Division of Policy and Planning and proper encryption is used.

8.4 **Restricted** or **Sensitive** information is **never** to be stored on cloud services without prior authorization from the Privacy Officer or Division of Policy and Planning and proper encryption is used.

8.4.1 Examples of cloud storage and services that **are not approved**, and must be approved beforehand include, but not limited to:

- Dropbox
- Microsoft One Drive (including One Drive for business)
- Google Drive
- Google Docs
- File Den

8.5 The use of personal storage, equipment, or personal storage for **Restricted** or **Sensitive** information is **strictly prohibited**. Any exception to this must have prior authorization from the Privacy Officer or Division of Policy and Planning, approved virus protection, and proper encryption.

8.6 Never share **Restricted** or **Sensitive** information without the proper authority, data sharing agreements, or memorandum of understanding documents in place.

9. Policy Specific Definitions

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

9.2 Restricted Data – Information that is legally protected (ex: Student educational records) or otherwise deemed by a qualified expert to be unsuitable for open access.

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

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

10. Enforcement and Authority

Enforcement of this policy is the responsibility of the Executive Vice Chancellor of Administration for the Commission and Council or his/her designee.

Any user found to have violated this policy may be subject to disciplinary or corrective actions based upon the policies, rules, and procedures of Commission and Council. These actions may include sanctions including, but not limited to, revocation of privileges up to and including termination of employment. Certain violations, misuse, or disclosures of confidential information may include civil and/or criminal penalties.

11. Change Log History

June 2019: New document;