DATA CLASSIFICATION AND PRIVACY MANAGEMENT POLICY

1. Purpose

This purpose of this policy is to establish and implement a framework and best practices for classifying, organizing, protecting, and accessing personally identifiable information (PII), the data collected and maintained by the West Virginia Higher Education Policy Commission (Commission) and the West Virginia Council for Community and Technical College Education (Council).

This policy is based on the 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]

2. Scope

This policy applies to all employees (interns, full-time, and part-time), 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 or the Council. Furthermore, this policy encompasses all data and information collected and maintained by the Commission or the Council, whether in electronic, paper, or other format, and regardless of the collection and storage method.

3. Authority

State and federal privacy laws and regulations
West Virginia Executive Order 3-17 (May 18, 2017)
The U.S. Department of Commerce's National Institute of Standards and Technology Special Publications (NIST SP) 800-14 and 800-53

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 if the data is mishandled.

[1] *State and Federal privacy laws and regulations include but are not limited to the following: W. Va. Code § 46A-2A-1, 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

A. **Restricted** data is the most sensitive to integrity and confidentiality risks. Data is classified as **Restricted** when unauthorized access or disclosure has the potential to cause harm to the individual, may violate State or federal privacy regulations, or may cause a data breach.

B. 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 **Restricted** data to perform their duties will be given access. **Restricted** data must be protected at the highest level possible.

C. Examples of **Restricted** data include, but are not limited to, 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 or federal-issued personal identification number, or driver's license number;
  - Bank account 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 or grade point average or ACT or SAT scores; and
  - Information included in the Free Application for Federal Student Aid (FAFSA) or financial aid information.
- Indirect PII is information, which, if linked, could be used to identify an individual:
  - Date or place of birth;
  - Business phone; and
  - Race/ethnicity.
- Computer vulnerability reports.

Level 2 – Sensitive

A. **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.

B. Direct access to **Sensitive** data is limited to authenticated and authorized individuals who require access to such data to perform their duties.

[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.*

Level 3 – Public

A. **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. If disclosed or shared, **Public** data would result in little or no risk to the individual or agency.

B. This type of information may be made public, published, or distributed without restriction in the form of physical documents, formal statements, press releasees, interactive data dashboards, or other publicly accessible means.

C. 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;
- Aggregate enrollment data;
- Agency public websites;
- Commission and Council policies and procedures.

5. Cloud Services

Any employee/division wanting to utilize a cloud computing service must complete the following:

- The requestor shall complete a privacy impact assessment as part of the purchasing process.
- The Privacy Team and/or the Division of Research and Analysis shall vet the request and determine that the cloud service meets agency standards and applicable privacy regulations.
- Any data collected by the Commission or the Council shall reside in the United States and be isolated so that other cloud customers sharing physical or virtual space cannot access the agencies' data or applications.
- The agencies' data shall 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.
- The agencies' data shall be encrypted at rest while in the cloud. Devices accessing the cloud storage shall be securely sanitized and/or destroyed at the end of their life cycle or if the device is lost or stolen.
- 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.
- In consultation with the agencies' General Counsel, the Privacy Team shall develop, and review documentation, contracts, and agreements to ensure compliance with State and federal laws.

6. Training and Awareness

Upon hire, all Commission and Council employees will receive the Confidentiality and Non-Disclosure Statement to review and sign. After the employee's execution of the Confidentiality and Non-Disclosure Statement, a member of the Privacy Team will schedule training with the employee to review the Data Classification and Privacy Management Policy.

All employees shall complete data security and/or privacy training periodically as required by the agencies.

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:

- **Level A – Extremely Critical:** These data and systems are critical to operations and must be protected by a plan allowing for 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.

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

- **Level C – Non-Critical:** These data and systems are necessary to the Commission and the Council, but short-term interruption or unavailability is acceptable.

8. General Safeguarding Policies

It is important to ensure that **Restricted** and **Sensitive** data are always protected. Users shall report immediately any privacy incident to the Privacy Team. Privacy incident 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. To prevent a privacy incident, users shall follow the below-listed procedures and use appropriate controls when sharing or accessing restricted or sensitive information.

There may be times when sharing **Restricted** or **Sensitive** information is necessary. In these instances, users shall contact the Privacy Team or the Division of Research and Analysis for assistance in determining the most secure method and processes to follow.

General Restricted or Sensitive Information Storage and Sharing Rules:

- Never email **Restricted** or **Sensitive** information.
- **Restricted** and **Sensitive** information shall be stored on the secure file folders assigned to

each user by the Senior IT Systems Administrator.

- **Restricted** or **Sensitive** information shall **never** be stored on local machines, smart phones, tablets, laptops, USB or flash drives, external hard drives, digital media, or other portable devices without prior written authorization from the Privacy Team or Division of Research and Analysis, who shall work with the user to ensure such information is properly encrypted.
- **Restricted** or **Sensitive** information shall **never** be stored on cloud services (Dropbox, Google Drive, Google Docs, File Den) without prior authorization from the Privacy Team or Division of Research and Analysis, who shall work with the user to ensure such information is properly encrypted.
- The use of personal storage or equipment for **Restricted** or **Sensitive** information is **strictly prohibited**. However, a user may request an exception to this prohibition from the Privacy Team or the Division of Research and Analysis, which shall only approve such request for good cause shown and which shall ensure that the user employs approved virus protection and proper encryption.
- Users shall not share **Restricted** or **Sensitive** information without the proper authority, data sharing agreements, or memorandum of understanding in place.

9. Definitions

9-1. Privacy Team – The Executive Vice Chancellor for Administration for the Commission and Council has appointed a Privacy Team and has designated them to establish and maintain a system of data privacy and information security and protection.

9-2. Reporting – Users shall report to or contact the Privacy Team via email: Privacy.Management@wvhepc.edu

9-3. 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

Any user who violates this policy may be subject to disciplinary action up to and including termination of employment. Certain violations, misuse, or disclosures of confidential information may also result in civil and/or criminal penalties.

Revised: February 2024