Policy No.: 8099
Board Approved: March 19, 2024
Revised:

Protection of Personally Identifiable Information (PII)

Hagerstown Community College (hereafter "the College") is committed to protecting the personally identifiable information (PII) of all students, employees, and any other individual whose PII is collected by the College in carrying out its mission.

This Protection of PII Policy is comprehensive in that it establishes overarching standards that affect a wide range of student and personnel records, information technology, and financial processes.

The purpose of this Policy is to provide a structure for and guidance about the protection of and access to sensitive data, information, and records in the possession of the College. The Director of Information Technology (DIT) and the Vice President for Finance are charged with overall PII management and enforcement.

I. Definitions for the Purpose of this Policy and Procedures

a. **"College Community"** refers to trustees, students, and all employees of the College as well as any independent contractors or other third parties to the extent articulated under contractual agreements.

b. **"Family Educational Rights and Privacy Act (FERPA)"** refers to a federal law protecting the privacy of student education records. The law applies to all schools receiving funds under any applicable program of the U.S. Department of Education.

c. **"Gramm Leach Bliley Act (GLBA)"** refers to a Federal law (primarily the Privacy Rule [16 CFR 313] and the Safeguards Rule [16 CFR 314]) requiring all financial institutions to develop, implement, and maintain safeguards to protect customer information. Because the College is in compliance with FERPA to protect the privacy of student records, the College is deemed to be in compliance with GLBA.

d. **"Individual"** refers to a person for whom the College collects PII.

e. **"Need to Know"** refers to the need for information in a record for the purpose of performing the required task(s) and responsibilities during the

course of an employee's job.

f. **"Periodic compliance checks"** refers to unscheduled inspections conducted by the DIT /DIT staff to examine whether safeguards are adequately protecting PII.

g. **"Personally Identifiable Information"** is a category of information linked to a specific individual that would allow a person, who does not have personal knowledge or the relevant circumstance, to identify the individual with reasonable certainty. Data elements that are considered PII include: an individual's name; the name of the individual's other family members; the address of the individual or individual's family; a personal identifier, such as the individual's social security number, identification number, or biometric record; financial data including student loans, banking information, credit card or credit information; other indirect identifiers, such as the individual's date of birth, place of birth, and mother's maiden name.

   Some information that is considered PII is available in public sources such as telephone books, public web sites, and College directories. Examples are: first and last name; address; work telephone number; email address; home telephone number; and general educational credentials.

   In contrast, other information like social security number, biometric data, financial data, date of birth are considered sensitive PII and have more stringent protection requirements.

h. **"Record"** refers to any educational information or data recorded in any medium.

i. **"Red Flags Rule"** refers to a federal regulation issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The Red Flags Rule requires financial institutions and creditors to implement a written Identity Theft Prevention Program and to provide for the continued administration of this Identity Theft Prevention Program. The College is subject to this rule because it holds student accounts that do not require full payment at the time of enrollment, and because it administers student loans.

j. **"President's Executive Leadership Team (PELT)"** refers to the President's Senior Leadership Team

II. Required Strategies for the Protection of Personally Identifiable Information

a. **Minimizing PII Use**

PII has the potential to subject individuals and/or the College to risk if inappropriately accessed, used, or disclosed. When use of PII is requested, the DIT will evaluate the context of use and determine if the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated is appropriate and aligns with this policy.

b. **Categorizing PII**

PII has the potential to subject individuals and/or the College to risk if inappropriately accessed, used, or disclosed. When use of PII is requested, the DIT will evaluate the context of use and determine if the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated is appropriate and aligns with this policy.

c. **Collection and Storage of PII**

Prior approval is required from the DIT to collect and/or store PII data on any device or system.

d. **Evaluation of PII Use**

When evaluating a request to use PII, the following factors must be considered:

1. The purpose of the data collection and how it is categorized
2. Whether there is another source of pre-existing data (reduction of duplicative information);
3. Whether all information requested is required (minimizing collection to only what is required);
4. How the data are being stored, for how long, and in what state (physical location, type of device, encryption, and retention);
5. How the data are being transmitted (if applicable) and in what state (encryption);
6. Whether agreements bind the College with third parties (software, services, web applications or forms); and
7. Whether the use of the PII has been vetted and approved by DIT or DIT staff.

e. **Administrative Safeguards**

Administrative safeguards include pertinent policies/guidelines developed to safeguard PII and training to increase awareness of and compliance with policies and guidelines related to safeguarding PII.

Administrative safeguards are created to ensure the College complies with the protection of PII in general, FERPA, and by extension the GLBA,

and the FTC Red Flags Rule.

f. **Technical Safeguards**

Technical safeguards include the development of information technology policies and guidelines, and implementation of tools to monitor and control access to PII, and strategies to retain and back up critical PII.

Technical safeguards, wherever possible, are treated as confidential to limit exploits that might lead to unintended or malicious exposure of PII.

g. **Physical Safeguards**

Physical safeguards include the development of standard operating procedures to provide physical control and destruction of PII, including but not limited to access control, secure storage facilities, shred bins, and surveillance in support of physical security for PII.

Physical safeguards, wherever possible, are treated as confidential to limit exploits that might lead to unintended or malicious exposure of PII.

h. **Employee Training**

Annual Cybersecurity training (which includes PII training) is required of all employees.