Policy No.: 8098
Board Approved: March 19, 2024
Revised:

Information Security Program Policy

Hagerstown Community College (hereafter "the College") is committed to ensuring that the operation of its information technology systems meet the necessary security controls and standards that provides reasonable protection for the confidentiality, integrity, and availability of data for which the College is responsible. The College will maintain and update the Information Security Program (hereafter "ISP"), as outlined below, to addresses the most current standards and to reasonably mitigate foreseeable risk. The ISP will be updated to comply with laws and regulations, to include, but not limited to, FERPA*, HIPAA*, PCI*, and GLBA*.

A. The College's ISP outlines the overall security posture and access control of College data. The ISP will also indicate who is responsible for data; all HCC employees with access to data are responsible for maintaining the integrity of that data by taking reasonable precautions to mitigate outside access. HCC data security and access is primarily the responsibility of that data's respective department leaders. The IT Senior Director is responsible for the overall security of College data, systems, and networks.

B. The College's ISP shall maintain a record of administrative, technical, and physical controls used to safeguard data information technology networks. The ISP will include, but is not limited to:

    - An outline of methods used to provide security, confidentiality, integrity and accessibility of systems and data
    - Categorization of data
    - List of personnel/organizations responsible for data
    - Steps taken to reasonably mitigate risk
    - Required legal and regulatory controls
    - Incident response procedure
    - Cybersecurity awareness training

C. In the event there is a valid justification to deviate from established controls, the Senior Director of Information Technology will review, document and provide final approval for waiving the requirement based on the requirements established within the ISP.

D. *Data Breach Notification* and *Data Breach Response Process are* provided in the guidelines developed by and housed within the IT Department which prescribe the required actions the College must take in addressing the unauthorized acquisition of computerized data.

E. The College will require Information Technology Security Awareness Training to be completed by all faculty and staff annually which will provide a common understanding of data privacy expectations, raise awareness of legal and regulatory responsibilities, and provide best practices to curtail inadvertent violations of

sensitive information. Circumstantial security training, retraining, and other security training may be required in addition to the annual training.

F. The Senior Director of Technology will ensure the ISP is updated regularly, as well as coordinate and facilitate the IT functions required to meet all county, state and federal technology audit responsibilities.

G. The IT Senior Director will provide the College's Board of Trustees an annual update with an overview of the ISP.

H. Excepting legal necessity, the ISP will not override any established Policies of the College. Other data and computer policies include, but may not be limited to Policies: 5056 - Telework Policy; 5093 - Use of Computing, Network and Communications Resources; 8073 - Information Technology Security; 8075 - Information Technology Hardware and Software.

* Acronyms

FERPA – Family Educational Rights and Privacy Act of 1974

HIPAA – Health Insurance Portability and Accountability Act of 1996

PCI – Payment Card Industry (Data Security Standard)

GLBA – Gramm–Leach–Bliley Act, (AKA: Financial Services Modernization Act of 1999)