6510 – Data Stewardship Policy

Policy Owner: Chief Information Officer
Associated Procedure: TBD
Date Adopted: October 19, 2021
Date Last Amended: N/A
Date Last Reviewed: October 19, 2021

Maintaining the confidentiality, security, and availability of College data is critical to the success of Harford Community College ("College"). This policy establishes the methodology by which the College will manage its data and assigns responsibilities for the control and appropriate stewardship of College data. The policy ensures that data access restrictions are based on legal, ethical and practical considerations; and informs stewards and custodians of College data of their responsibilities.

The College expects all stewards, custodians and users of its College data to manage, access, and utilize this data in a manner that is consistent with the College's need for security and confidentiality. College data is owned by the College and should be shared appropriately to meet the needs of the College and its customers. The College functional areas must develop and maintain clear and consistent procedures for access to College data.

Definitions:
- **College Data:** Items of information that are collected, maintained, and utilized by the College for the purpose of carrying out administrative and academic operations. College data may be stored either electronically or on paper and may take many forms. It may be stored on or off campus, locally generated or acquired from an external service.
- **Data Steward:** College administrator or designee having direct operational-level responsibility for data assets in their area including data security and quality.
- **Data Custodian**: A department and/or personnel responsible for providing a secure infrastructure in support of the data including providing access to users

as authorized by the Data Stewards; and implementing and administering appropriate levels of controls over the information.

- **Data User:** An individual who creates and uses College Data as part of their assigned duties or in fulfillment of assigned roles or functions within the College community. Any College employee with access to College Data can be considered a Data User.
- **Data Classification:** A grouping of data for risk management and security purposes based on its level of sensitivity and the impact to the College should the data be disclosed, altered or destroyed without authorization.

Roles and Responsibilities

All College employees, students and affiliates granted access to College Data are responsible for understanding the terms and conditions under which they may access and use College Data. An individual may have one or more of the roles listed below.

Data Steward

- Will have broad-based knowledge of the data for which they are a steward and encompass all uses of that data as viewed from the College's perspective.
- Understands how their data is used in all information systems.
- Will assign appropriate classification to College data. The College has adopted three primary classifications: restricted, sensitive and public.
- May assign administrative and operational responsibility to specific employees or groups of employees.
- Defines appropriate use of assigned data types. Some data types may be used by multiple areas and any changes should be coordinated with other Data Stewards.
- Understands all legislation that regulates data class use.
- Reviews and approves users' access to data.
- Reviews and updates user access routinely and communicates changes to Data Custodian.
- Assists in establishing necessary security and access controls for data.

Data Custodian

- The Information Technology department is the trusted custodian of the data on behalf of the college.
- Provides and removes user access to data as defined by the Data Steward.
- Provides a secure and stable environment for storage of the data.
- Defines requirements for safeguarding data and ensures that security policies are implemented.

Data User

- Protects all data and access to data in their care. Recipients of *Restricted Data* are responsible for maintaining the restricted nature of the data.
- Uses data and access to data only as required in the performance of legitimate College functions and their job.
- Adheres to applicable Federal and State laws, requirements of any applicable contracts, and College policies, standards and procedures.