



6515 –Data Classification and Handling Policy

Policy Owner: Chief Information Officer

Associated Procedure: TBD

Date Adopted: March 8, 2022

Date Last Amended: N/A

Date Last Reviewed: March 8, 2022

Information is a valuable asset and is critical to the mission of the College. Determining how to protect and handle information depends on the following considerations: information's type, importance, and usage. Classification is necessary to understand which security practices should be used to protect different types of information; the more protected the information needs to be, the more practices are required.

The policy applies to all College employees and other covered individuals (e.g., affiliates, vendors, independent contractors, etc.) in their handling of College data, information, and records in any form (paper, digital text, image, audio, video, etc.) during the course of conducting College business (including but not limited to administrative, financial, instruction, or service).

Definitions:

- **College Data:** Items of information that are collected, maintained, and utilized by the College for the purpose of carrying out College business. 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.
- **Confidentiality:** Access to information must be strictly limited to protect the College and individuals from loss.



- Data Handling: Includes, but is not limited to, the following: Creating, collecting, accessing, viewing, using, storing, transferring, mailing, managing, preserving, disposing, or destroying.
- Users: Includes all members of the Harford Community College community to the extent they have authorized access to College information resources and information systems, and may include students, faculty, staff, contractors, consultants, temporary employees, and volunteers.
- 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.

All College information whether at rest (i.e., stored in databases, tables, email systems, file cabinets, desk drawers, etc.) or in use (i.e., being processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.) must be handled according to the data classification levels described in the associated procedures.

Determining classification levels should be done according to an assessment of the need for confidentiality of the information.

Limiting access to authorized individuals/entities/devices ensures legal obligations are fulfilled and/or protects the College and its stakeholders from the disclosure of data that is sensitive in nature.

All individuals covered under this policy are required to handle College information per the procedural controls found in the Data Classification and Handling Procedures.