POLICY Board of Trustees – Montgomery College 66005

Chapter: Fiscal and Administrative Affairs Modification No. 001

Subject: Data Asset Management and Security

I. The Board of Trustees recognizes that data asset management is an essential part of fulfilling the College's mission. Data asset management promotes strategic decision-making, student success, institutional sustainability, and good stewardship by providing a single source of truth and a more consistent user experience to internal and external audiences.

II. The purpose of this policy is to govern the confidentiality, integrity, availability, ethical use of and quality of College data to drive evidence-based decision making, to assign responsibilities for the control and appropriate stewardship of College data, and to support and maintain related policy principles and procedures.

III. It is the policy of the Board of Trustees that data is an institutional asset and will be managed according to a Collegewide data governance framework to facilitate the mission and activities of the College and minimize exposure to risk inherent in information management. Data asset management provides oversight and vision to institutional data and the information systems, software, and hardware that makes data assets available. No individual or unit owns any data elements. It is owned and managed by the College, and not tracked in silos.

IV. Data shall be collected in a lawful, ethical, and appropriate manner in accordance with the requirements of applicable laws and regulations (e.g., FERPA, GDPR, PCI, etc.).

V. This policy creates, under the authority of the President, a data governance framework to support the consistent and appropriate management of College information.

VI. The College will provide education programs to employees and students to heighten awareness of the critical value of College data, the need to protect it, and its use in data-informed decision-making.

VII. The president is authorized to establish procedures necessary to implement this policy.

____

____

Board Approval: **____, 2022**

PROCEDURE - Montgomery College **66005CP**

Chapter: Fiscal and Administrative Affairs Modification No. 001

Subject: **Data Asset Management and Security**

I. Definitions

A. College Data ("Data"): All Data, regardless of its origin within the College, that is used by or belongs to the College, or that is created, processed, stored, maintained, transmitted, or copied using College IT Resources. For the purpose of this procedure, the terms "data" and "information" are used interchangeably. They include any information kept in print, kept electronically, kept as test Data in a non-production system, or kept audio-visually, whether stored onsite or offsite, that meets any of the following criteria:

1. Created or updated via the use of the College's Systems of Record or used to update Data in the Systems of Record;

2. Acquired or maintained by College employees in performance of official administrative or academic job duties;

3. Relevant to planning, managing, operating, or auditing a major function at the College;

4. Included in College administrative reports or College records.

B. Data Classification (per College Procedure 66002CP): An assigned classification to Data defined as below:

1. Confidential (High Risk): Data and systems are classified as high risk if:

a. Protection of the data is required by law/regulation, or

b. Montgomery College is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed; or

c. Any Data that could, by itself, or in combination with other such data, be used for identity theft, fraud or other such crimes; or

d. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

e. Examples of confidential Information includes but are not limited to the following: the personnel record of any past or present employee; any record containing PII; credit or debit card data; student information which has not been identified as directory information (see Board Policy #41003 Student Cumulative Records); records or material that have otherwise been identified as confidential, subject to trademark or a copyright protection, or for which there is a contractual limitation on disclosure; records of the Office of General Counsel, or any records of which exposure unnecessarily invades personal privacy or impairs individual rights.

2. Sensitive (Moderate Risk): Data and systems are classified as moderate risk if they are not considered to be confidential and high risk and:

   a. Data that is not protected by regulatory requirements, but is considered internal use only, or

   b. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.

   c. These Data might include, but is not limited to, employee, academic, planning, facility, emergency or administrative Data that is restricted for reasons related to public or individual safety, competition, ongoing development or is otherwise sensitive in nature.

   d. Examples include employment Data, financial transaction Data and purchasing Data.

3. Public (Low Risk): Data and systems are classified as low risk if they are not considered to be moderate or high risk, and:

   a. The data is intended for public disclosure, or

   b. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

   c. Examples include Press Releases and Course Schedule and Directory Information (as defined in Board Policy #41003).

C. Data Access: The rights to read, enter, copy, query, download, upload, test or update Data. The scope of Data Access allowed to any Data User will vary given their academic or business need and may change from time to time. Users with access to Confidential or Sensitive Data will take training as established by the College and will execute required confidentiality agreements.

D. Data Access Provisioning: The processes established for requesting, granting, and terminating permission to access Data in the Systems of Record or other approved Data stores.

E. Data Set: A collection of related College information that supports the College mission or activities.

F. Data Security: Processes that administer and monitor Data Access and, consistent with laws and industry standards, protect the confidentiality, integrity and availability of Data.

G. Data Trustees: College administrators who have responsibilities for major data management decisions to include oversight of the implementation and verification of processes for Data privacy, protection, access, and accountability. Data Trustees may designate appropriate personnel to complete processes required under this Procedure.

H. Data Stewards: Subject matter experts about the data utilized in their unit or area, who can provide background on current and future data needs for that unit. Data Stewards are appointed by their respective Data Trustees.

I. Data Stewardship: The responsible oversight of a data set, including principal responsibility for the establishment of standards and guidelines for appropriately managing and securing that data across the College.

J. Data Users: Individuals with authorized access to use Data as part of their assigned duties. Individuals who have access to Data are in a position of special trust and as such are responsible for protecting the security and integrity of that Data. Data Users can be employees, contractors or any role given access to Data.

K. Information Technology Resources ("IT Resources"): IT resources include all electronic equipment, facilities, technologies, and data used for information processing, transfer, storage, display, printing, and communications by Montgomery College or its Users. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, modems, email, networks, telephones, voicemail, facsimile transmissions, video, multi-function printing devices, mobile computer devices, data, multimedia and instructional materials. This definition also includes services that are owned, leased, operated, provided by, or otherwise connected to Montgomery College resources, such as cloud computing or any other connected/hosted service provided. (see College Procedure (AUP)).

L. Least Privilege: The privacy and security objective of granting Data Users access to Data in the most restrictive set of privileges needed to perform their assigned duties. It further includes specific activities, technical processes and written processes that enforce and secure the minimal set of privileges.

M. Personally Identifiable Information (PII): Data that can be used, in part or in combination with other Data to distinguish or trace an individual's identity, such as name, social security number, date of birth, student/staff M number; and any other information that is linked or linkable to an individual, such as medical, educational, financial, or employment information.

N. System Administrator: A system administrator is an employee or contractor who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. It includes system administrators, database administrators, network administrators, web administrators, desktop administrators and Office of Information Technology support staff.

O. Systems of Record: Software applications that act as central collegewide repositories of business activities. This specifically includes human resources, payroll, financial management; student admissions, schedules, grades, counseling, financial aid, alumni records; advancement records; library patron activity; e-mail; and student learning systems.

II. Data Governance

A. Data governance is a cooperative effort; the success of data governance efforts depends on collaboration between key College stakeholders, who provide critical expertise and perspectives related to specific aspects of data management and security, and the College community.

1. Data trustees provide a strategic perspective on data governance. They direct institutional data initiatives and ensure that data is used in support of the College's mission, vision, and strategic goals.

2. Data stewards provide an operational perspective on data governance. They oversee efforts to ensure and improve the informational quality, effectiveness, usability, strategic value, access to, and security of data. They also understand how their data is managed and used across the institution.

3. Data custodians provide a technical perspective on data governance. They manage information systems and shared data repositories on behalf of data trustees and data stewards. They also understand the underlying infrastructure that supports the management and security of data across the institution.

B. The President and/or the Chief Analytics and Insights Officer will establish and oversee the Data Trustees Council (DTC).

1. Data Trustees Council (DTC): Membership of the DTC will be composed of, but not limited to, the Data Trustees, appointed by the Chief Analytics and Insights Officer in consultation with each senior vice president and the president's office, and the chairs of the Data Stewards Committee (DSC) and the Data Security Advisory Committee (DSAC). It is charged with setting institutional priorities of data quality and data driven decision making. The DTC will have the authority, interest, and resources necessary to:

a. Define management responsibilities around various data sets.

b. Create and track actions related to data.

c. Oversee data stewardship efforts for the College information entrusted to their care.

d. Identify and work to eliminate silos and barriers to data management throughout the College.

e. Recommend institutional policies, procedures, standards and guidelines for the storage, accessibility, and management of institutional data.

f. Appoint representatives to the DSC and DSAC.

g. Ultimately be accountable for their functional area's compliance with policies, laws, regulations, standards, and guidelines for the appropriate management of College information.

h. Provide clarification and conflict resolution about data management.

2. In addition, there will be two operational sub-committees to assist with data Governance:

a. Data Stewards Committee (DSC): The DSC will be represented by Data Stewards, identified by their respective Data Trustees, and is charged with

1) Oversee the informational quality, effectiveness, usability, strategic value, and security of the College information within their stewardship.

2) Establish definitions of the data sets within their stewardship.

3) Develop and promulgate data management standards and guidelines to ensure the confidentiality, integrity, availability, and usefulness of College information within their stewardship.

4) Ensure that College information within their stewardship is managed according to legitimate interests and operational requirements and in a manner that ensures the privacy and security of that College information.

5) Develop and publish standards and guidelines for access to College information within their stewardship.

6) Review and approve uses or proposed uses of College information within their stewardship.

7) Authorize the creation of shared data repositories containing College information within their stewardship and assign custodianship responsibilities for those shared data repositories.

8) Authorize the access of individual end users to College information within their stewardship.

9) Audit at least annually the authorized access to College information within their stewardship.

b. Data Security Advisory Committee (DSAC):The DSAC will be composed of the IT Policy Administrator (ITPA), and representatives appointed by the Data Trustees.

The DSAC will have the authority, interest, and resources necessary to:

1) Assist the EAC and DSG in the implementation of the risk management aspects of this policy.

2) Create and maintain appropriate guidance documents or resources (i.e. Data Classification Matrix) to help Data Users more fully differentiate between Confidential, Sensitive and Public information, as well as approved storage of the data classes.

3) Assist data stewards in coordinating initiatives to improve the confidentiality, integrity, and availability of College information across the College and its units.

4) Aid in the development of standards and guidelines concerning the management of information security and risk by the College and its units.

5) Report to the DAMC relevant security initiatives and recommendations as appropriate.

6) Enforce and clarify Data Classification, Access, Authentication and Storage of College Data.

7) Serve as liaison between the College community and the Office of Information Technology.

3. In the event of a conflict with College Policy and Procedure 66002, the ITPA will have the authority to make final decisions in the interest of data protection.

III. Education

Education is a key element of this Policy. The College will provide education and information, as appropriate, for students and employees to enhance understanding and increase awareness of the College's Data Asset Management Policy and these Procedures. Any mandatory education requirements will be announced and posted on the College's website. The President is authorized to provide institutional leadership and guidance for developing education programs to increase knowledge and share information and resources to prevent violations of this policy and procedure. Some goals to be achieved through education are: (a) notifying individuals of conduct that is proscribed; (b) informing employees, students, and other members of the college community, including contractors, about the proper way to recognize and address complaints involving a violation of this Policy; and (c) preventing issues that this Policy addresses.

____

Administrative approval: **_______, 2022**