POLICY Board of Trustees – Montgomery College 66002

Chapter: Fiscal and Administrative Affairs Modification No. 002

Subject: Confidential Data Management and Security

I. The Board of Trustees hereby authorizes the president to promulgate procedures and create programs to appropriately manage receipt, creation, copying, transmittal and use of certain confidential data in College operations by College employees and contractors. This policy and procedures hereunder are intended to address the increased regulatory attention to certain classes of data that are received, created, and maintained by the College. These data pose increased risks to persons and College operations that are the subject of or rightful users of, that data when such data are subject to unauthorized access or use by third persons. The purpose of these actions by the College are to further limit, to the extent possible, access and use of such data by unapproved or illicit third persons with the attendant risk of misuse and damage to the College community and College operations.

II. To comply with applicable contracts and state and federal laws, and to protect the College community, the College has the right and obligation to receive, store, maintain, manage, secure, and use certain confidential data pertaining to individuals, including students, customers and employees. Although these data may be in various paper copy forms or electronic media forms, they may be readily transferred, transmitted or copied into various other forms. Current electronic media forms and networks through which they may be accessed require additional actions to properly steward and manage them securely.

III. It is the policy of the Board of Trustees to safeguard sensitive hard copy and electronic data and to restrict individual access to such data only as it is necessary to perform the functions required by their position at the College and in accordance with state and federal laws. Individual access will be determined by appropriate authorization of both the individual’s supervisor and the owner of the data. Those individuals, supervisors and owners are responsible for the College data stored, created, processed and/or transmitted under their care and for following the security requirements established under this policy.

IV. The College will protect confidential data in its possession through a tightly controlled process that may include the following:

A. Systematic and continuous review and identification of various classes of data created, accessed, maintained, and transmitted by the College, separating these classes of data into level of confidentiality categories ~~(e.g., Highly Sensitive, such as social security numbers, bank and credit card information that are associated with identity theft or are otherwise highly regulated in their use and access; Very Sensitive, such as personal information in addition to Highly Sensitive information, and Sensitive, such as certain other information that may be confidential under such laws as the public information act)~~.

B. Provision of various levels of access, creation and use controls that may require appropriate access/creation authorization by a small group for various classes of data, and then only on a need to know or use basis.

C. Provision of special controls on creation or copying of various classes of data to locations that may be accessed outside of the College's firewall and specification of network uses.

D. Requirements of specific security for certain classes of data, including locked file cabinets for hard copies, encryption for electronic versions, limitation of conversion keys to limited persons (such as permitting broad use of ―M‖ numbers for students and employees, but limiting conversion keys of these numbers to social security numbers to a small group of employees that can further ensure proper use of these Highly Sensitive data).

E. Confirmation of the Red Flag Program followed by the College and further refinement of the program to ensure its effectiveness in current operations, to ensure full compliance with the Fair and Accurate Credit Transactions Act of 2003 that requires rules to protect against identity theft protection.

F. Integration of applicable security requirements into employee performance expectations and job descriptions, and proper enforcement of those expectations.

G. Review and change of access, creation, maintenance and transmittal authorization upon a change of status or position of each employee.

H. Special security requirements as may be appropriate for maintenance or use of confidential data outside of the College's secure facilities and networks, including but not limited to home pc's, mobile computing and storage devices and paper files taken home or elsewhere outside of College facilities. This may include encryption and other security precautions, as well as limitations on transmissions and copying.

I. Integrate and coordinate this policy with policies and procedures pertaining to confidential information and records management, as well as employee responsibilities.

V. Information systems that store, process or transmit sensitive electronic data will be minimized and consolidated to eliminate storage of data that is not properly authorized. All information systems and sensitive electronic data, throughout its lifecycle, will be secured in a manner that is reasonable and appropriate, given the level of confidentiality, value and criticality that the data has to the College and to its constituents.

VI. The College will provide education programs to employees and students to heighten awareness of the critical need to protect College confidential data.

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

Board Approval: June 18, 2012**; ____, 2022**

PROCEDURE - Montgomery College 66002CP

Chapter: Fiscal and Administrative Affairs Modification No. 0**02**

Subject: **Confidential Data Management and Security**

I. Definitions

A. College Data (“Data”): All Data 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 official College administrative reports or official College records.

B. ~~College Data Coordinating Group: Collegewide group convened periodically by the Information Technology Policy Administrator (ITPA), comprised of selected College leadership. The group’s role is to review institutional data management, privacy, and security activities and provide recommendations to ensure processes are effective and relevant to maintaining data privacy and security~~ **Data Trustees Council (DTC): Data governance group composed of 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.**

C. Confidential Information: Confidential Information includes but is 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.

D. 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 Level 1 or Level 2 Data will take training as established by the College and will execute required confidentiality agreements.

E. 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.

F. Data Classification~~ Definitions~~: An assigned classification to Data defined as below:

1. **Confidential (High Risk) – Level 2: Data and systems are classified as high risk if:**

    a. Protection of the data is required by law/regulation; and
    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 identify 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.

    ~~Level 1 - Highly Sensitive: Data that is protected by federal, state, or local law or regulation, College Policy or Procedure, professional code, contract; or other binding mechanism. This includes PII and Confidential Information. Any Data that could, by itself, or in combination with other such data, be used for identity theft, fraud or other such crimes should be treated as Highly Sensitive Data. Examples include Social Security numbers, Credit Cardholder Data ("CHD") numbers and student records.~~

2. ~~Level 2 – ~~Sensitive **(Moderate Risk) – Level 1: Data and systems are classified as moderate risk if they are not considered to be confidential and high risk if:**

    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.

    ~~Data that is not protected by regulatory requirements, but is considered internal use only. This 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. Examples include employment Data, financial transaction Data and purchasing Data.~~

3. **Public (Low Risk) – Level 0: 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, course schedules, and directory information (as defined in Policy/Procedure 41003/41003CP-Cumulative Student Records).

~~Level 3 - Not Sensitive/Public: Data approved for distribution to the public without restriction. Its distribution is without potential hazard to the College, affiliates or individuals. Examples include Press Releases and Course Schedule and Directory Information (as defined in Board Policy #41003).~~

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

H. 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** ~~officials who have responsibilities for major data management decisions within their academic and/or administrative area 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~~.

I. 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.

J. 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 ~~Any and all parts of the College's network, computing hardware, storage, software, mobile computing or telephone devices, or related peripherals such as printers and scanners that are administered, allocated and managed by and for the College either on-site or at a College administered location, or remotely at College-approved external locations and by College-approved vendors and providers of cloud-based services. This includes devices not owned by the College but that are connected to the college network and/or any related peripheral devices~~.

K. 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.

L. 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.

M. 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.

N. 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 Security Requirements.

A. Security Requirements for Level **2** ~~1~~ - ~~Highly Sensitive/~~Confidential:

1. The highest level of Data Security applies to Level **2** ~~1~~ Data.

2. The principle of Least Privilege applies to Level **2** ~~1~~ Data.

3. Data Users with access to Level **2** ~~1~~ Data are approved and periodically recertified by the appropriate Data Trustee or designee.

4. Data Users with access to Level **2** ~~1~~ Data will have their privileges revoked upon the termination or any change of the employment/contractual access that necessitated the Data Access.

5. Data Users with access to Level **2** ~~1~~ Data will not store, process or share

such Data outside of a System of Record or the College network without approval of appropriate Data Trustee, or, in the case of group access requests for a large Data extract, by the appropriate Data Trustee and the **IT Policy Administrator** (ITPA).

6. Data Users that have received approval to store or process Level **2** ~~1~~ Data outside of the Systems of Record may only perform these actions on IT Resources, devices or applications that are approved as meeting Data Security requirements under these Procedures or more specifically as set forth by the ITPA or the appropriate Data Trustee.

7. CHD will not be stored on any College system, including any Systems of Record or any type of internal or external storage. Data Users with access to CHD will process CHD only in accordance with Office of Information Technology and Office of Business Services standards and processes. No credit card transactions may take place over any College network or system unless properly encrypted and approved by the Office of Business Services and the ITPA in advance.

B. Security Requirements for Level **1** ~~2~~ – Sensitive:

1. A level of Data Security commensurate with the sensitive nature of this Level **1** ~~2~~ Data applies to this Data.

2. The principle of Least Privilege applies to Level **1** ~~2~~ Data.

3. Data Users with access to Level **1** ~~2~~ Data are approved by a Data Trustee and periodically recertified.

4. Data Users with access to Level **1** ~~2~~ Data will have their privileges revoked upon the termination or any change of the employment/contractual access that necessitated the Data Access.

5. Data Users with access to Level **1** ~~2~~ Data will not store, process or share such Data outside of the Systems of Record without approval of the ITPA and the Data Trustee.

C. Security Requirements for Level **0** ~~3~~ - ~~Not Sensitive/~~Public:

While Level **0** ~~3~~ Data is available to the Public, a minimum level of control is required to prevent unauthorized modification or destruction of this Data.

III. Roles and Responsibilities

A. Vice President of Instructional and Information Technology/Chief Information Officer (“VP/CIO”):

1. Oversees the management of the College’s Systems of Record, Data Access, Data Security and management processes.

2. Serves as the mediator for discrepancies between assigned roles and helps establish balance between the aspiration of private and secure Data

management practices and the interests of efficient and informed College operations.

B. Data Trustees:

1. Periodically affirm that Data Access is current.

2. Review Data technology requests that include a substantial movement of Level 1 and/or Level 2 Data that requires the Data to be extracted from the Systems of Record and stored elsewhere (either onsite or offsite). The VP/CIO or designee must approve any such request.

C. ITPA:

1. Will periodically ~~convene the College Data Coordinating Group to~~ review institutional Data management, privacy and security activities and provide recommendations to **the Data Trustees Council to** ensure these Procedures are effective and relevant to maintaining Data privacy and security.

2. Verifies appropriate Data Access Provisioning of requested Data Access to Level 1 or Level 2 Data.

3. Works within IT and collegewide to implement appropriate security standards for IT Resources associated with all Data.

4. Creates appropriate guidance documents or resources to help Data Users more fully differentiate between Level **0, 1, and 2** ~~1, 2, and 3~~ Data, as well as approved storage of the Data types.

IV. Uniform Data Management

A. Systems of Record Data Storage Primacy:

1. All College Data will be contained in or directly accessible to the College's Systems of Record, unless specifically exempted by the CIO for storage in other approved Data stores such as cloud-based storage services. Any such exempted Data stores outside the Systems of Record will be inventoried and must meet the requirements defined in this procedure.

2. Security and Data Access controls will be available and implemented to protect Data from disclosure based upon the location and usage, as well as the different levels of Data Classification.

3. College Data contained in paper form should be secured with appropriate physical security standards.

B. E-mailing Data:

1. College Data sent within or attached to an e-mail to a party outside of the College e-mail system will be properly secured consistent with the sensitivity of the information and Least Privilege.

2. Level 1 or 2 Data in retained or archived e-mails will be managed in accordance with the College's record retention policy.

C. Imaging Data:

1. Imaging of paper College documents will be performed using IT Resources.

2. Imaged Documents should be redacted of unnecessary Level 1 Data to the extent reasonably possible and consistent with operational and legal needs.

3. Imaged Data will be retained or deleted consistent with the College's record retention policy.

D. Local Data Storage on Devices:

1. Electronic storage of Level 1 or Level 2 Data outside of a System of Record on College owned workstations or mobile devices (devices including but not limited to laptops, tablets and smartphones) will be approved by the CIO or designee and the appropriate Data Trustee.

2. No storage of Level 1 or Level 2 Data may take place on non-College owned devices.

3. No storage of Level 1 or Level 2 Data may take place on an externally based file hosting service unless it is an IT Resource.

4. Data Users, when required, will execute appropriate confidentiality agreements regarding the Data.

5. When the storage of or access to Level 1 or Level 2 Data is approved for a College-owned device, then the devices storing the Data will meet certain system Data Security requirements, including but not limited to:

a) Reasonable physical security.

b) College supported file and/or disk encryption should be utilized, consistent with Office of Information Technology requirements.

c) Operating system software will be patched and up to date.

d) Anti-Virus software will be installed and up to date.

e) The user may not operate their device using an account with administrative privileges, unless required by the user's job function.

f) Authentication to these devices will be consistent with IT Authentication Standards.

g) The device will be configured to lock after a reasonable period of inactivity, consistent with Least Privilege.

h) Mobile devices owned by the College will be returned to the College for a verification of current technology as deemed necessary by the Office of Information Technology; and

i) If the device is a mobile device, it will also contain appropriate security safeguards to ensure Least Privilege.

V. No Third Party Rights; No Expectation of Privacy

A. While these Procedures promote the privacy and security of Data, they do not create any consumer, customer, student, or other third-party rights or remedies, or establish or increase any standard of care that would otherwise not be applicable.

B. The College does not, by inclusion of certain Data with Level 1 or Level 2 classification, intend to create any individual expectation of privacy where none would otherwise exist.

VI. IT Resource Eligibility

A. The scope of access to and use of IT Resources will vary in accordance with the affiliation of a user and may change from time to time. The College establishes processes and standards for verifying the eligibility of persons seeking to access and use College IT Resources and Data.

B. The scope of access and use granted will be consistent with these Procedures.

C. Eligibility to use College technology resources will cease when the user no longer has an affiliation that supports eligibility. Processes consistent with this Procedure will disable and ultimately delete College granted accounts and reimage College IT resources.

D. The eligibility of all individuals for an IT Resource may be tested periodically against official College sources, including employee, faculty, and student records. Other sources may be used where these records do not accurately reflect ongoing affiliation.

E. Data Access to Level 1 or Level 2 Data given to temporary employees (including student employees and contractors) will expire automatically on reasonable time periods consistent with business need. Data Access needed beyond the initial period will require a new consent.

F. Data Access to Level 1 or Level 2 Data to permanent employees will be recertified periodically in methods consistent with Office of Information Technology processes.

G. Group shared storage devices will be provided to users consistent with current technology and business needs. Group shared storage devices are meant to be used for active business Data and not for long-term storage. Group shared storage devices will be periodically reviewed, and files not in active use, as determined by the ITPA, will be deleted.

VII. 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 Confidential Data Management and Security 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: November 27, 2017**; _______, 2022**