POLICY Board of Trustees – Montgomery College 66002

Chapter: Fiscal and Administrative Affairs Modification No. 001

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