Office of
Information
Technology

IT Program

NETWORK AND INFORMATION SECURITY AND PRIVACY PROGRAM

Original Effective Date:	11/30/2009
Last Revised:	2/27/18
Last Reviewed:	04/01/2020
Next Scheduled Review Date:	04/01/2023
Version No.:	2.1
Contact:	Information Security and Privacy Director

PURPOSE

Information assets of Montgomery College ("College"), in all its forms and throughout its life cycle, will be protected through information management standards and actions that meet applicable Federal, state, regulatory, or contractual requirements and support the College's mission, vision, and values. It is the intent of the Office of Information Technology (OIT) that through a layered combination of technology, standards and education the risk of attacks and incidents can be significantly reduced to a manageable level.

SCOPE

The scope of this Network and Information Security and Privacy Program ("Program") is to delineate the areas of responsibility that exist under College and legal requirements and the IT Standards, Processes, Procedures, Guidelines, Specifications and FAQs ("IT Standards") that respond directly to those College requirements.

PROGRAM

THEREFORE, OIT WILL UTILIZE REASONABLE STANDARDS, PROCESSES, AND TECHNICAL MEASURES TO MEET THE COLLEGE REQUIREMENTS, INCLUDING THE FOLLOWING:

A. **Privacy Obligations and Responsibilities**: The College has a number of obligations and responsibilities in relation to privacy. The principles of confidentiality, integrity and availability of College information runs through every effort so that information is properly protected from exposure; that information cannot be changed in any form, and that information is available to those who have a need for access. Privacy requirements of the Federal Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCIDSS) and as established by Data Classification needs of the College.

B. **OIT Organizational Controls and Resources:** The IT Standard Development Process will ensure that Standards emanating from all areas of the OIT are properly developed, vetted, and implemented, consistent with a coordinated approach to problem solving. Consideration of resources will always be considered.

C. **Program Coordinators:** The Information Security & Privacy Director ("ISPD") is designated as the Policy Coordinator of this Program. The IT Security Manager ("ISM") is designated as the Technology Coordinator of this Program reporting to the Information Security and Privacy Director. This Program is meant to provide guidance and standards for reasonably securing all College information assets.

D. **IT Standards Management:** OIT should have in place appropriate IT Standards to ensure a safe, compliant, and properly risk-managed computing and network environment and to meet the College requirements. The Information Security and Privacy Group ("ISP") of the OIT will act as project manager in the development of IT Standards requested and developed within OIT in collaboration with the College, and in concert with appropriate working groups. The development of IT Standards will comply with the IT Standard Development Process. The primary focus of the

Standard Development Process is to create a plan approved by the appropriate administrator and complete the plan in accordance with time limits also determined by that administrator.

E. **Acceptable Use.** "All users who request and/or are given access to College-owned and operated information technology resources agree to use those resources in a manner consistent with the mission of the College and in compliance with Board of Trustees' policies, as well as all applicable laws, procedures, rules and regulations" (Acceptable use Policy). It is understood that actions taken on an IT resource (e.g., computer system, College application or system, etc.) belongs to the owner of the specific user ID under which those actions take place.

F. **Information Identification and Classification:** OIT will work with individual College units/departments to help them identify the information assets they control, the level of protection necessary to protect information depending on how it is classified, and what access to data is necessary to support their business processes. Different levels of security and access need to be determined for each level of data sensitivity within the College. The current or residual use of Personally Identifiable Information ("PII") needs to be examined and eliminated where it does not support the College Mission or a properly secured business function.

G. **Risk Assessment and Risk Management:** The OIT will reasonably work with individual College departments to help them determine and manage the risks of handling information. Risk assessment is an important part of any information security process and will help in assigning priorities for implementing controls, mitigating risk, and accepting risk. Risk assessment can be both a survey-based risk assessment, as well as application-based risk assessment for all College units and departments, with a key element being the identification of practices, access and processes surrounding both PII and sensitive information generated at and held by the College.

H. **Account Creation.** OIT will reasonably review procedures for establishing on-line accounts, determining levels of approval, accessing confidential information, granting remote access, monitoring inactive accounts, resetting passwords, and closing accounts based on voluntary leave, change of duty, termination, or change in contractors/vendors.

I. **Identification and Authentication.** To safeguard critical application systems, information, and networks from unauthorized access or intrusions, OIT implement identity and authentication of a user/customer before granting access to resources and services by implementing reasonable authentication methods.

J. **Security Awareness:** OIT will review and implement programs that help train College Users to be aware of their roles and responsibilities and of the security risks. These College-wide security and privacy awareness training and education programs should rely on as many existing communication tools, information sharing venues, publications, College websites, and campus publications that make sense to leverage.

K. **Network Security:** OIT will deploy multi-layered protection at the Internet gateway, on the internal network, on network servers, and at the desktop level to prevent introduction of malicious code or unauthorized access into the College's information systems. The **ITSG** will always review current protection methods and the maturity of security efforts.

L. **Access Control.** Consistent with College policy, OIT will work with College Users to implement appropriate measures that should be taken when using technology resources to ensure the confidentiality, integrity and availability of College sensitive information, and that access to sensitive information is restricted to authorized users. Specific to information systems should be implemented with access controls that provide for the assurance that only persons with a need can access specific information. This concept of "least privilege" assures individuals or College departments only have access to that information required in order to perform a job or complete a business process.

N. **Workstation/Endpoint Security.** OIT will implement security into each individual computing system or device that acts as a network client and serves as a workstation or personal computing device, including laptops and other mobile devices, and those individual computing systems in open laboratory and library work areas.

O. **Backups of Networked Data.** OIT will develop reasonable procedures ensuring networked information, including desktops, maintained by the College is backed up. Backups will allow the College to recover from interruptions in service in a timely manner and to restore critical information and services. Backup frequency and method shall be determined and implemented according to College business needs and in line with higher education industry standards.

P. **Development, Installation, and Maintenance of Systems:** OIT development, installation , and maintenance reflects requirements that help to ensure sound operation of IT resources through secure development and installation practices. Installation and changes to IT resources will be introduced and implemented in a controlled and coordinated manner.

Q. **Physical Security:** OIT should have appropriate physical security for facilities housing IT personnel and systems, as well as critical information systems and information assets wherever they may be located (whether in the primary Network Operations Center (NOC) at TPSS, any other local NOC, any communication wiring closets or other areas containing OIT equipment or controlled by OIT. Departments other than OIT which house critical IT Systems or critical information should be protected commensurate with the risk presented.

R. **Incident Response:** OIT will establish and maintain a security incident response capability. Properly prescribed response measures can provide mitigation of harm, quick remediation, and opportunities to improve information security controls for the College and possibly others who could be affected by an incident.

S. **Data Protection.** OIT will periodically review its methods of data protection, including the various devices that hold data, as well as how such data is stored. Devices may include devices resident in the NOC or POP, on the network, desktops or on more personal use devices such as laptops, tablets, cell phones, home computers used in the performance of duties, USB devices or any other devices on or in which data may be stored. Data encryption will be considered when feasible and as appropriate.

U. **IT Assets.** The OIT must manage its software and hardware assets appropriately, in a manner that ensures control and tracking of all assets at any given moment.

V. **Legal Compliance.** The OIT will work with College departments as a resource to help ensure compliance with existing information security requirements, whether required by laws or by contract, including but not limited to FERPA, PCIDSS and GLBA.

STANDARD NUMBERING

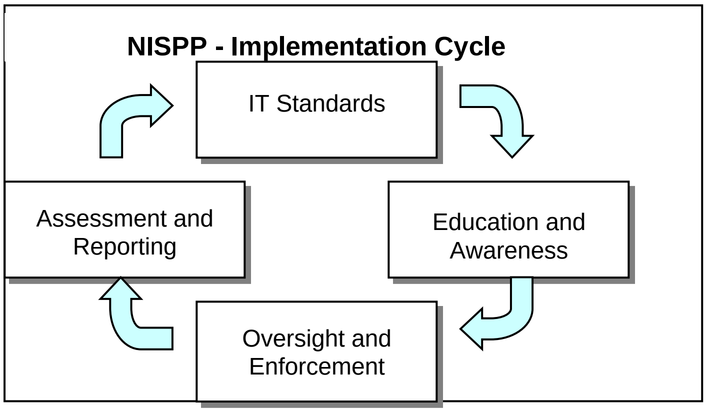
Standards, processes, procedures, specifications and plans will be numbered in an orderly manner to represent this Program's subject matter area (listed below) so that individual Standards etc. can be easily identified. The format for the Standard identification number is: IT##001, IT##002, etc. where ## refers to the number of the subject matter area. Documents related to a standard (i.e., processes, procedures and guidelines) will use the Standard identification number followed by A, B, C, etc.: IT##001A, IT##001B, etc.

1. OIT Organizational Controls and Resources.
2. IT Standards Management.
3. IT Standards Hierarchy and Process.
4. Data Stewardship/Data ownership.
5. Information Identification and Classification.
6. Risk Assessment and Risk Management.
7. Account Creation.

8. Identification and Authentication.
9. Security Awareness.
10. Network Security.
11. Access Control.
12. Workstation/Endpoint Security.
13. Backups of Networked Data.
14. Development, Installation, and Maintenance of Systems.
15. Physical Security.
16. Incident Response.
17. Data Protection.
18. Business Records Management/Retention.
19. IT Assets.
20. Legal Compliance.
21. IT Infrastructure
22. Electronic Communications

IMPLEMENTATION OF THIS PROGRAM

The implementation of this Program will not consist of distinctly separated processes, but instead represents a flow of activities that yield an ever-maturing Program. The implementation cycle involves establishing IT Standards, educating the user community about their roles and responsibilities, governance structures to ensure compliance, and monitoring/reporting of progress. Information security is not a one-time project, but an ongoing process that is the shared responsibility of the College.



AUTHORITY FOR THIS PROGRAM

Acceptable Use Policy and the accompanying Procedure/Guidelines Statement

66002 Confidential Data Management and Security

WEB SITE ADDRESS FOR THIS STANDARD

APPROVALS / REVISION HISTORY

DATE	VERSION / REVISION / NOTES	APPROVER
November 30, 2009	Original roll-out of this NISSP document.	Patrick Feehan, Information Security and Privacy Director/ITPA
February 27, 2018	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson