Monroe Community College
STATE UNIVERSITY OF NEW YORK

7.3 Information Technology Security Policy

Category: Technology
Name of Responsible Office: Technology Services
Title of Responsible Executive: CFO and Vice President, Administrative Services
Date Established: October 3, 2013
Date Last Approved: March 7, 2022

Policy Statement

The purpose of this Information Security Policy is to clearly establish the role of Monroe Community College in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables Monroe Community College to implement a comprehensive system-wide Information Security Program.

Background

This policy will assist the college in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. The policy is based on a nationally recognized framework, NIST 800-53, provided by the National Institute of Standards and Technology (NIST), and consists of eighteen (18) separate policy areas, with supporting Standards documents. Most other security laws, mandates and contractual requirements are mapped back to NIST 800-53.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides comprehensive governance to addresses key controls in all known areas needed to provide for the confidentiality, integrity, and availability of the college's information assets. This framework also provides administrators with the guidance necessary for making prioritized decisions.

Monroe Community College needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill the college's mission. The Information Security Program must be risk-based, and risk treatment decisions must be made based on addressing the highest risk first.

Monroe Community College's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to organizational limitations and resource constraints. The college must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

Scope

The scope of this policy includes all information assets governed by the college. All personnel and service providers who have access to or utilize information assets of the college, including data at rest, in transit or in process shall be subject to these requirements. This policy applies to:

- All information assets and Information Technology (IT) resources operated by the college;
- All information assets and IT resources provided to the college through contracts, subject to the provisions and restrictions of the contracts; and
- All authenticated users of Monroe Community College information assets and IT resources.

Information and System Classification

Monroe Community College must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

Provisions for Information Security Standards

The Monroe Community College Security Program is framed on National Institute of Standards and Technology (NIST). Monroe Community College must develop appropriate control standards and procedures required to support the college's Information Technology Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Monroe Community College Security Program is based on NIST Special Publication 800-53. This publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

The current Information Security Standards may be found in the MCC Protocols.

Access Control (AC)

Monroe Community College must limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and Training (AT)

Monroe Community College must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of college information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and Accountability (AU)

Monroe Community College must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

Assessment and Authorization (CA)

Monroe Community College must: (i) periodically assess the security controls in its information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in college information systems; (iii) authorize the operation of the college's information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration Management (CM)

Monroe Community College must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency Planning (CP)

Monroe Community College must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the college's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and Authorization (IA)

Monroe Community College must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Monroe Community College information systems.

Incident Response (IR)

Monroe Community College must: (i) establish an operational incident handling capability for college information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate college officials and/or authorities.

Maintenance (MA)

Monroe Community College must: (i) perform periodic and timely maintenance on college information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Media Protection (MP)

Monroe Community College must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) encryption, where applicable, (iiii) sanitize or destroy information system media before disposal or release for reuse.

Physical and Environmental Protection (PE)

Monroe Community College must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning (PL)

Monroe Community College must develop, document, periodically update and implement security plans for college information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

Personnel Security (PS)

Monroe Community College must: (i) ensure that individuals occupying positions of responsibility within organizations are trustworthy and meet established security criteria for those positions; (ii) ensure that college information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with Monroe Community College security policies and procedures.

Risk Assessment (RA)

Monroe Community College must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage or, transmission of organizational information.

System and Services Acquisition (SA)

Monroe Community College must: (i) allocate sufficient resources to adequately protect college information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third- party providers employ adequate security measures, through federal and state law and contract, to protect information, applications and/or services outsourced from the organization.

System and Communications Protection (SC)

Monroe Community College must: (i) monitor, control and protect college communications (i.e., information transmitted or received by college information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within college information systems.

System and Information Integrity (SI)

Monroe Community College must: (i) identify, report and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within college information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Program Management (PM)

Monroe Community College must implement security program management controls to provide a foundation for the organizational Information Security Program.

Privacy

Monroe Community College must make every reasonable effort to respect a user's privacy. However, personnel do not acquire a right of privacy for communications transmitted or stored on college resources.

Additionally, in response to a judicial order or any other action required by law or permitted by official college policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the

organization, the VP Administrative Services, or an authorized agent, may access, review, monitor and/or disclose computer files associated with an individual's account.

Enforcement

Monroe Community College may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security or functionality of college and computer resources.

Exceptions

Exceptions to the policy may be granted by the VP Administrative Services, or his or her designee. Exceptions must be reviewed annually.

Responsibility

Associate Vice President/CIO

Contact Information

Technology Services