Monroe Community College
STATE UNIVERSITY OF NEW YORK

7.3 Information Technology Security Policy

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

Summary

This information technology security policy establishes the overall intent of Monroe Community College to support and promote information security in all its practices. This policy and supplemental procedures, requirements and guidelines will support the College's effort to ensure the basic security elements of confidentiality, integrity and availability.

Policy

Policy Statement

Monroe Community College will establish information technology security standards for all information assets and systems under the College's control and for the personnel who access these assets and systems. Adherence to these requirements ensures that Monroe Community College protects its information assets with due diligence, complies with government regulatory and contractual requirements and meets industry best practices for this protection.

Background

The ability for the college to meet the daily needs of the academic and administrative communities is facilitated, in large part, through the use of information technology systems. While critical to the business of the college, these technologies also introduce risks. The risks and corresponding threats associated with IT are increasing in both number and variety. The advent of hacking tools and persons willing to distribute viruses and malicious code has increased the risks to IT organizations and the assets they are charged to safeguard. Overall system integration and interconnectivity, college systems and networks are increasingly at risk to intrusions, misuse of data, and other attacks from both internal and external sources. Monroe Community College must secure its information and technology systems and provide its faculty, students and staff with clear education and direction for the safeguarding of college information assets. This direction extends to contractors or other authorized agents with access to college information technology resources, data or assets.

Responsibility

The CFO/Vice President, Administrative Services will manage the Information Technology Security Policy. Execution of the Policy through procedures, requirements and guidelines will be the responsibility of the CFO and Vice President of Administrative Services, and the Director of Communications and Network Services.

Contact Information

Office of Administrative Services

Related Information

College Documents

- Attachment 1 – Information Technology Security Procedures
- Attachment 2 – Information Technology Security Requirements

Reference Documents

- SUNY Information Security Guidelines – Part I: Campus Programs and Preserving Confidentiality (SUNY Policy Document #6608).
- SUNY Information Security Guidelines – Part I: Campus Programs and Preserving Confidentiality (SUNY Policy Document #6608) Appendix G: Information Security Practices Recommended by New York State.
- New York State Personal Privacy Protection Act (PPPL) and SUNY Compliance Document #6603.
- SUNY Information Security Guidelines – Part I: Campus Programs and Preserving Confidentiality (SUNY Policy Document #6608) Appendix F: Confidential Practices and Procedures in New York State Policy.
- New York State Office of Cyber Security, Cyber Security Policy P03-002 Information Security Policy.