Monroe Community College
STATE UNIVERSITY OF NEW YORK

4.4 Cyber Security Awareness and Education Policy

Category: Technology
Name of Responsible Office: Administrative Services
Title of Responsible Executive: CFO and Vice President, Administrative Services
Date Established: October 2, 2017
Date Last Approved:

Summary

Computer security is not just about keeping systems and networks secure. It is also about the people who use those systems and how their behaviors can lead to cyber exploitation. Proper training can reduce the number of people who do careless things that cause a security incident or breach.

Training and education must be ongoing due to the ever-increasing variety and sophistication of cyber threats. These include but are not limited to spam, phishing, spoofing, malware, and ransomware, which can result in identity theft, data corruption, loss of intellectual property, operational disruption, and damage to the reputation of the institution. By law, MCC is liable for losses, fines and penalties caused by data breaches, on top of the internal costs for incident investigation and remediation. Moreover, loss of trust in the College's ability to protect the personal information of stakeholders could result in reductions in donations, grant funding, and student enrollment.

Policy

Policy Statement

All employee users will be required to complete regular training. In addition to annual training, College-wide awareness campaigns will be ongoing, via MCC Daily Tribune articles, newsletters, screensavers, webcasts, videos and other means. The awareness and education program will include the following:

- Ongoing assessment of user compliance with cyber security standards
- Remedial training for those found not practicing good cybersecurity defenses
- ~~Feedback surveys to improve the awareness training and education programs~~

Training completion results will be maintained by the Chief Information Security Officer.

Enforcement

Users who fail to demonstrate a good faith effort to comply with cyber security standards may be required to change their password at more frequent intervals than normal. Additionally, persons routinely or egregiously in violation of security standards and procedures resulting in risk or harm to the College's information security are subject to a range of restrictions in order to protect MCC information systems and data. This includes but is not limited to the loss of PC administrative rights and / or the loss of network access privileges.

Applicability

This policy applies to all members of the College community with **employee access** to the College network resources.

Definitions

Users – Any person who has an MCC Network Account with **employee level permission** to use network resources.

Responsibility

CFO/Vice President, Administrative Services

Contact Information

Office of Administrative Services

Related Information

SUNY Information Security Policy 6900

SUNY Information Security Guidelines: Campus Programs & Preserving Confidentiality