Monroe Community College
STATE UNIVERSITY OF NEW YORK

4.4P Cyber Security Awareness and Education Procedure

Category: Technology

Name of Responsible Office: Technology Services

Title of Responsible Executive: CFO and Vice President, Administrative Services

Date Established: January 7, 2020

Date Last Approved:

This procedure serves to guide how the college will administer annual cyber security awareness training for information technology users with employee level access. The primary mode of training is an online vendor solution hosted by SUNY using federated authentication.

Description of Procedure

I. **Training Program**:

a. Prior to fall semester, the training system's online training modules are reviewed and selected by the CISO for the upcoming academic year.

b. The annual training is rolled out in October, which is Cyber Security Awareness Month.

i. Users are instructed by an automated email to take the designated annual training, which is securely accessed through a link in myMCC. Once this training is successfully completed, the user has fulfilled their annual training requirement, unless they click on a test phishing email.

ii. Periodic simulated phishing emails are sent from the system to employees to gauge their skill level. Employees 'clicking' on links or opening attachments in the simulated phishing tests are assigned additional refresher training.

II. **Communications**:

a. CISO informs executive team via email about the upcoming rollout of the annual cyber security training program in advance of employee communications.

b. Articles informing employees about the cyber security training program and its upcoming launch are posted to the Daily Tribune prior to the annual rollout of Cyber Security Training.

c. A welcome message is sent from the CISO informing each user that they have been enrolled in annual cyber security awareness training. This message is sent via an email originating from the training system. Existing users receive the welcome email when the annual training campaign starts in October. Employees hired after the start of the campaign receive the welcome email when their MCC employee account is activated.

d. Information regarding cyber security is disseminated using the Daily Tribune throughout the academic year by the CISO. Tribune articles include updates, scam alerts, tips, thanks, reminders, and notifications of deadlines for completion of training and consequences of non-compliance.

e. Reminder messages are sent out periodically via the training system to individuals who have not started or have not completed their training.

III. **Online training system user loads**:

a. Banner is the primary source for the users loaded into the system.

b. Users are selected to be included if they have an active job (for faculty, staff, and administrators), are assigned a course (for adjuncts), or are non-employees who have been granted an employee level account.

IV. **Compliance**:

a. The consequence for users not completing the annual training by the deadline is the expiration of their network ID password every seven days until they submit proof of training completion to the Technology Support Team.

b. The frequent password expiration mitigates risks posed by untrained users.

Definitions

User with employee level access: User with an employee email and/or network ID.

CISO: Chief Information Security Officer

Related Information

College Documents

4.4 Cyber Security Awareness and Education Policy

External Documents

None