A-18b PROCEDURE Cyber Security

Objective:
Reduce the College's risk of a data breach and other cybercrimes through education and awareness. Protect PII and other sensitive information contained within College systems as implemented by the Information Services division.

Activation:
SCC Employees have the following requirements on an annual basis:

1. Regular and temporary employees with an FTE factor equal to or greater than 0.75 must complete one cyber security awareness training per fiscal year. If needed, individuals will be provided with additional training immediately following a failed phishing test.

2. Individuals requesting access to the SCC network via VPN access will complete cyber security training and be enrolled in the SCC Multi-factor authentication group.

3. Part-time regular employees, with an FTE status of less than 0.75, must complete one cyber security awareness training per fiscal year.

4. Part-time temporary employees with an FTE status of less than 0.75, including adjunct, are invited and encouraged to complete one cyber security awareness training per fiscal year.

The following job roles are required to have multi-factor authentication:

- All users on the Administrative team
- All users with VPN access
- All users with Colleague NAE access
- All users with access to Financial or Financial Aid data
- All users with access to HR/personnel data

In situations where an employee has interacted with a real phishing scam or other cybercrime incident (not a training exercise), the Information Services team will:

1) Reset the individual's password to prevent unknown entities from logging into the SCC network.

2) Automatically enroll the individual in additional cyber security awareness trainings that must be completed within 7 days of enrollment.

3) If the individual has VPN access, that access will be temporarily deactivated until the additional training is completed.

4) If the individual is not enrolled in SCC's Multi-factor authentication group, they will be required to set up multi-factor authentication to help prevent potential future login attempts from unknown entities.

The Information Services division will track the completion of all cyber security education and protocol.

Related Policy/Procedure: A-18, A-18a
Adopted: 1/27/20
Reviewed:
Revised:
Web link:
Tags: cyber security, cyber security education, multi-factor authentication