# Information Security Awareness Training Policy

**POLICY**
Information Security Awareness Training Policy

**POLICY CATEGORY**
Information Technology Services

**PURPOSE**
STCC has a responsibility to implement information security best practices and to comply with federal and state laws and regulations related to Information Security Awareness Training.

The purpose of this policy is to educate users on their responsibility to help protect the

all personnel are trained on relevant rules, regulations, and best practices for cybersecurity.

**SCOPE**
This policy applies to all STCC employees (Non-Units, MCCC, AFSCME, and part-time) including: staff, administration, full and part-time faculty, adjunct faculty, seasonal, temporary, casual, interim, student workers, interns and volunteer employees and covers all offsite locations.

**POLICY**
The AVP/Chief Information Officer shall implement an enterprise-wide information security awareness training program and develop appropriate training modules in collaboration with the Director of Infrastructure and Security, AVP of Human Resources and Legal. The training course will be administered through the KnowBe4 web-based learning platform.

<u>Annual Information Security Awareness Training:</u> All **NUP** personnel will be required to complete annual Information Security Awareness Training before December 1, 2021, and annually each year thereafter. **All MCCC, AFSCME, and part-time** personnel will be required to complete annual Information Security Awareness Training before November 1, 2022, and annually every November thereafter. Automatic email reminders and alerts will be sent to personnel (1) month prior to the annual course completion deadline.

The program will include annual training and/or refresher courses for NUP personnel.

The training shall:

- Explain acceptable use of information technology

- Inform users about relevant policies and standards and risks to information systems that house STCC data assets
- Educate users on cyber security topics, including but not limited to:

  Virus or malicious software (Malware)
  Phishing attempts
  Social engineering
  Application / Operating system vulnerabilities

  Include periodic phishing training and remedial education as necessary.

The awareness program shall be updated regularly by the Director of Infrastructure and Security to align with organizational policies and procedures, and shall be:

- Built on lessons learned from information security incidents and emerging threats
- Ensure that all principles, policies, procedures and training materials are accessible by all personnel as appropriate.

Completion rates will be tracked and reported to division VP/Deans/supervisors and AVP/Chief Information Officer.

<u>New Hire Security Awareness Training:</u> All newly hired personnel must complete an initial Information Security Awareness Training course. This course shall be conducted