

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING PROCEDURE	Procedure 8.09.01
--------------------------------------	--	----------------------

I. PROCEDURE STATEMENT

Southwestern Community College ("College") shall implement a Security Awareness Training Program designed to educate and inform users about cybersecurity threats and the necessary measures to protect information systems. This program will be reviewed and updated annually to reflect the latest threats and changes in technology.

II. SECURITY AWARENESS TRAINING PROGRAM

- A. **Mandatory Training:** All new employees, contractors, and relevant stakeholders must complete initial security awareness training as part of their onboarding process.
- B. **Recurring Training:** All employees, contractors, and stakeholders must complete annual security awareness training. This training shall be refreshed yearly to include new and emerging cybersecurity threats.
- C. **Training to Recognize Social Engineering Attacks:** The IT Division will utilize simulated phishing tests, which replicate actual attack techniques, to educate employees on recognizing and avoiding suspicious emails and to improve overall threat identification and response effectiveness. This training will be, at a minimum, conducted annually.
- D. **Specialized Training:** Additional role-based training will be provided to those in roles with elevated access privileges or security responsibilities.

III. DOCUMENTATION AND RECORD-KEEPING

The College's Information Technology Division shall maintain records of all completed security awareness training sessions, including the names of participants, the dates of training, and the content covered. These records shall be kept for a minimum of three years.

IV. COMPLIANCE

Failure to complete the required security awareness training within the designated timeframe will result in the suspension of access to the College's information systems. Continued non-compliance may lead to disciplinary action, including termination of employment or contractual agreements.

V. RESPONSIBILITIES

- A. **Information Security Officer (ISO):** Responsible for the development, implementation, and oversight of the Security Awareness Training Program.
- B. **Supervisors:** Ensure that their team members complete all required training.
- C. **Employees and Contractors:** Required to complete training as specified and adhere to all security policies and procedures.

VI. REVIEW AND UPDATE

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING PROCEDURE	Procedure 8.09.01
--------------------------------------	--	----------------------

This procedure shall be reviewed annually by the Information Security Officer to ensure it remains relevant and effective in addressing current cybersecurity threats.

Legal References:

- Statewide Information Security Manual, NC Department of Information Technology, SCIO-SEC-302: Awareness and Training Policy
- CIS Controls v8, Control 14: Security Awareness and Skills Training
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations
- 1B SBCCC 700.3 - Community College System Cybersecurity Framework

Adopted: September 2025

Revised: N/A