SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATION SECURITY PROGRAM**	Procedure 8.10.01

I. SCOPE

This procedure applies to all College-owned information systems, data, and users, including employees, students, contractors, and third-party service providers. It encompasses all aspects of information security, including governance, risk management, incident response, and training.

II. DEFINITIONS

A. **Information Security Program (ISP):** A structured approach to managing the security of information systems and data to protect against unauthorized access, use, disclosure, disruption, modification, or destruction.
B. **Cybersecurity Incident:** Any unauthorized access to, use of, or disruption of information systems that threatens the confidentiality, integrity, or availability of the College's data.
C. **Data Classification:** The process of categorizing data based on its sensitivity and criticality to ensure appropriate levels of protection.

III. ROLES AND RESPONSIBILITIES

A. **Vice President for Information Technology:** Oversee the implementation and management of the ISP. Ensure alignment with the North Carolina Department of Information Technology's Statewide Information Security Manual.
B. **Campus Safety/Security:** Collaborate with the IT Division to integrate physical security measures with information security initiatives.
C. **IT Division:** Monitor and manage the security of the College's IT systems and data. Administer annual cybersecurity awareness training. Respond to cybersecurity incidents in collaboration with the North Carolina Department of Information Technology.
D. **Employees and Users:** Complete required cybersecurity awareness training annually. Report suspected cybersecurity incidents to the IT Division immediately.

IV. INFORMATION SECURITY FRAMEWORK

A. **Governance:** The College adopts the Statewide Information Security Manual as its principal cybersecurity framework, ensuring consistency with state policies and compliance with applicable laws.
B. **Risk Management:** The College will conduct regular risk assessments to identify vulnerabilities, evaluate threats, and implement appropriate mitigations.
C. **Data Protection:** All data will be classified and managed in accordance with *Policy 8.11 - Information Classification and Handling*.

V. CYBERSECURITY INCIDENT RESPONSE

A. **Prohibited Ransom Payments:** The College prohibits payments or negotiations with entities engaging in ransomware or other extortion-based cybersecurity incidents.
B. **State Consultation:** The College will consult with the North Carolina Department of Information Technology (NCDIT) regarding all cybersecurity incidents, ensuring compliance with state law and guidance.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATION SECURITY PROGRAM**	Procedure 8.10.01

C. **Incident Response Plan:** The IT Division will maintain and regularly update an incident response plan to address potential threats and incidents effectively.

VI. CYBERSECURITY AWARENESS TRAINING

A. **Mandatory Training:** All full-time and part-time employees must complete annual cybersecurity awareness training administered by the IT Division during the fiscal year.
B. **Enforcement:** Employees who fail to complete training will lose access to their accounts until training is completed. Continued non-compliance may result in disciplinary action, up to termination.

VII. ENFORCEMENT AND MONITORING

A. **Policy Violations:** Violations of this policy may result in disciplinary action, up to termination of employment or contract termination.
B. **Periodic Audits:** The IT Division will conduct regular audits to ensure compliance with the ISP and identify areas for improvement.

VIII. REVIEW AND REVISION

This policy will be reviewed annually to ensure alignment with evolving cybersecurity threats, regulatory changes, and institutional needs.

Legal References:

- North Carolina General Statutes, including Chapter 143 - Information Technology
- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 2 (Inventory and Control of Software Assets), Control 17 (Incident Response and Management)

Cross References:

- Policy 8.10 - Information Security Program
- Policy 8.11 - Information Classification and Handling
- Policy 8.20 - Data Management

Adopted: September 2025

Revised: N/A