SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **RISK MANAGEMENT**	Procedure 8.13.01

I. SCOPE

This policy applies to all College-owned information systems, facilities, data, and personnel, including contractors and third-party service providers. It encompasses risks related to cybersecurity, operational continuity, and compliance.

II. DEFINITIONS

A. **Risk Management:** The process of identifying, assessing, prioritizing, and mitigating risks to achieve organizational objectives.
B. **Risk Assessment:** A systematic evaluation of potential threats, vulnerabilities, and the potential impact on the organization’s assets.
C. **Mitigation Plan:** A documented strategy to address identified risks by implementing security controls or operational changes.

III. ROLES AND RESPONSIBILITIES

A. **Vice President for Technology:** Oversee the development and implementation of the risk management framework. Ensure alignment with state and federal regulations.
B. **IT Division:** Conduct regular risk assessments and manage mitigation plans. Maintain an inventory of assets to facilitate risk analysis. Monitor and report on emerging risks.
C. **Risk Owners:** Collaborate with the IT Division to address identified risks related to their areas of responsibility.
D. **Employees and Contractors:** Adhere to security policies and procedures to minimize risks. Report potential risks or vulnerabilities to the IT Division.

IV. RISK MANAGEMENT FRAMEWORK

A. **Risk Identification:** Regularly identify potential risks to information systems, facilities, and operations through assessments, audits, incident reporting, and annual penetration testing.. Include risks related to cybersecurity, operational disruptions, third-party services, and compliance violations.
B. **Risk Assessment and Analysis:** Conduct formal risk assessments to evaluate threats, vulnerabilities, and potential impacts. Assign risk levels based on likelihood and impact using a standardized scoring method.
C. **Risk Mitigation:** Develop mitigation plans for identified risks, prioritizing high-impact and high-likelihood risks. Implement security controls, operational changes, and training to address risks effectively.
D. **Monitoring and Reporting:** Continuously monitor identified risks and mitigation efforts. Report significant risks and mitigation statuses to College leadership quarterly.

V. ASSET MANAGEMENT

A. **Asset Inventory:** Maintain an up-to-date inventory of all information systems, hardware, software, and data repositories.
B. **Critical Assets:** Identify and prioritize critical assets requiring enhanced protection measures.

SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **RISK MANAGEMENT**	Procedure 8.13.01

VI. THIRD-PARTY RISK MANAGEMENT

A. Conduct due diligence for all third-party vendors and contractors to ensure compliance with College security policies.
B. Include security and risk management requirements in contracts and service agreements.
C. Monitor third-party performance to ensure ongoing compliance.

VII. COMPLIANCE REQUIREMENTS

Risk management activities must comply with the following:

- North Carolina Statewide Information Security Manual.
- CIS Controls v8, including Control 3 (Data Protection) and Control 15 (Service Provider Management).
- Applicable federal regulations, such as FERPA and GLBA, and FTC Safeguards

VIII. ENFORCEMENT

A. Employees and contractors who fail to adhere to risk management policies and procedures may be subject to disciplinary action, up to termination of employment or contract termination.
B. The IT Division will conduct periodic audits to ensure compliance with this policy.

IX. REVIEW AND REVISION

This policy will be reviewed annually or as needed to address evolving threats, regulatory changes, or operational requirements.

Legal References:

- North Carolina General Statutes, including Chapter 143 - Information Technology
- Statewide Information Security Manual, NC Department of Information Technology
- CIS Controls v8, Control 1 (Inventory and Control of Enterprise Assets) Control 3 (Data Protection), Control 15 (Service Provider Management), Control 18 (Penetration Testing)
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations

- FTC - Safeguard Rules Title 16, Chapter I, Subchapter C, Section §3.14.4

Cross References:

- Policy 8.10 - Information Security Program

Adopted: September 2025

Revised: N/A