Committee Meeting: Policy & Governance Committee	Date: January 12, 2026
Committee Chair: Melodie Baker	
New or Edited: New	

POLICY NAME: Security Risk Management

POLICY TYPE: Managerial

SUBMITTED BY: Daniel Bartkowiak, Information Security Officer

ISSUE OR STATEMENT OF PURPOSE: The purpose of this policy is to establish a comprehensive information security risk management framework that enables SUNY Erie Community College ("SUNY Erie" or "the College") to identify, assess, mitigate, and monitor risks to its information assets, in alignment with SUNY policies and applicable regulatory requirements.

The Security Risk Management policy has been created in response to the adoption of the new SUNY 6900 Information Security Policy and the development of SUNY Erie's own Information Security Policy (ISP). Historically, the Acceptable Use Policy (AUP) served as the sole ITS policy governing user behavior across SUNY Erie. With the introduction of the ISP, ITS has decided to create the Security Risk Management policy to enforce provisions and processes in the ISP, writing them for improved clarity, and incorporating new provisions to address emerging technologies.

NEW OR EDITED POLICY: New

POLICY:

Scope:

This policy applies to all SUNY Erie workforce members, including employees, contractors, consultants, vendors, volunteers, and any third parties with access to SUNY Erie systems, data, or facilities. It includes all information systems and assets owned, managed, or operated by SUNY Erie, whether on-premises, cloud-hosted, or managed by third-party service providers.

Definitions:

Non-Directory Information: Student or institutional information protected under FERPA, GLBA, NYS regulations, or SUNY policy that is not publicly releasable without authorization.

Risk: The potential for loss, damage, or negative impact resulting from a threat exploiting a vulnerability.

Vulnerability: A weakness in systems, processes, or controls that could be exploited.

Sensitive Data: Information classified as Moderate or High according to the SUNY Data Classification Standard.

Critical Systems: Systems essential to academic or administrative operations, including systems that store, process, or transmit regulated or sensitive data.

Vendor: Any third-party organization or individual providing products, software, or services to SUNY Erie involving access to SUNY Erie data, systems, or networks.

Risk Appetite Statement:
SUNY Erie adopts a conservative risk appetite regarding the confidentiality, integrity, and availability of its information systems. Any identified High-risk item requires explicit acceptance by Executive Leadership. High-risk items include, but are not limited to:

- Expose regulated or sensitive information;
- Significantly disrupt academic or administrative operations;
- Violate federal/state laws or SUNY policies;
- Create unreasonable operational, financial, or reputational impact.

Institutional Security Principles:

SUNY Erie is committed to protecting its information assets and ensuring the confidentiality, integrity, and availability of institutional data. All College units share responsibility for managing security risks in accordance with SUNY policy, NYS law, and industry standards.

The College will:

- Conduct regular risk assessments.
- Implement appropriate risk mitigation strategies.
- Maintain a formal risk register.
- Monitor the effectiveness of corrective actions.
- Ensure compliance with SUNY's Information Security Policy, Acceptable Use Policy, Access Management Policy, and related policy and standards.

Information Security Risk Management Framework:

The College will maintain a formal Security Risk Management Framework that includes:

1. Risk Identification – Identifying threats, vulnerabilities, and risks to institutional systems.
2. Risk Analysis & Evaluation – Assessing likelihood, impact, and prioritization.
3. Risk Response – Selecting mitigation, transfer, avoidance, or acceptance strategies.
4. Monitoring & Review – Ongoing tracking of risks, controls, and remediation.

System Categorization:
SUNY Erie will categorize systems using SUNY's impact scale (Low, Moderate, High) consistent with the SUNY Data Classification Policy. Categorization will inform control requirements and risk prioritization.

Risk Assessment Requirements:

- Risk assessments must be performed by ITS or qualified third parties.
- Conducted for new systems and major system changes (major = changes affecting authentication, data flows, integrations, external access, or security-relevant configuration).
- Business continuity takes priority when major changes are discovered after deployment.
- Assessments must consider threats, vulnerabilities, and vendor risks.
- Results must be documented in TDNext or another approved system of record.
- Findings must be included in a plan of action and milestones.

Risk Register:
ITS will maintain an official risk register owned by the Information Security Program Lead.

- The register must track risks, owners, remediation, and status.
- A written summary will be provided to Executive Leadership at least annually.

Asset Inventory:

ITS will maintain an inventory of all critical assets, including:

- Servers, network systems, and applications.
- Systems storing or transmitting sensitive or regulated data.
- Backup and recovery systems.

Documentation of unsupported systems and deprecated protocols.

Vendor Risk Management:
Vendor Review Requirements:

- Only vendors accessing or handling sensitive or regulated data require formal security review.
- Vendors must complete the appropriate SUNY Erie External User Access Agreement or Vendor Access Agreement.
- Vendors must provide a completed HECVAT and, if available, any SOC 2 Type II, ISO 27001 reports, or equivalent third-party audit documentation; providing these materials generally requires a signed NDA.
- Cloud vendors must align with the SUNY Cloud Security Policy.

Ongoing Oversight:

- Vendor risks must be reassessed at least annually.
- ITS will track vendor remediation requirements and maintain documentation.

-

Assessment & Authorization:
ITS will implement continuous assessment and authorization activities:

- Periodic security assessments to evaluate control effectiveness.
- Plan of Action and Milestones (POA&M) to track corrective actions.
- Annual validation of compliance with SUNY standards.
- Documentation of authorization decisions and residual risk acceptance.

Exceptions:
Exceptions to this policy may be approved only by the Information Security Program Lead and Executive Leadership.

- Exceptions must be documented using SUNY Erie's Exception Management Procedure.
- All exceptions must be reviewed annually.

Enforcement:
Failure to adhere to this policy may result in:

- Suspension of system access;
- Revocation of vendor access
- Disciplinary action in accordance with the Acceptable Use Policy and Code of Conduct.

Roles & Responsibilities:

Information Security Program Lead: Oversees framework, maintains risk register, performs assessments.
Information Technology Services (ITS): Conducts reviews, evaluates vendors, manages remediation.
Executive Leadership: Approves High-risk exceptions in partnership with the Information Security Program Lead.
Procurement: Ensures system and vendor acquisitions are routed through ITS.
Legal Counsel: Assists in reviewing contractual risk language when necessary.
Vendors: Comply with all SUNY Erie security requirements as stated in the SUNY Erie vendor agreement after submission.
All Workforce Members: Protect institutional data and report risks or incidents.
Review and Revision:

This policy will be reviewed at least annually by the Information Security Program Lead and updated to reflect changes in technology, SUNY policy, or regulatory requirements.

DOES IT SUPERCEDE A POLICY/WHICH ONE (if so, attach redline version):

POLICY & GOVERNANCE COMMITTEE RECOMMENDED ACTION:
Policy & Governance Committee recommends the Board of Trustees accept the Managerial policy under Committee Briefings, Policy and Governance Committee. This Policy supersedes all prior policies/procedures and practices related to Information Security Policy.

DATE OF BOARD ACCEPTANCE: January 29, 2026

POLICY & GOVERNANCE COMMITTEE TEAM FOLLOW-UP:
Following Trustee acceptance, this Managerial policy will be included in the SUNY Erie Community College Managerial Policy Manual.

INFORMATION/INPUT CONSIDERED DURING POLICY & GOVERNANCE COMMITTEE DELIBERATIONS:

1. SUNY Information Security Policy
2. SUNY Data Classification Standard
3. SUNY Cloud Security Policy
4. Acceptable Use Policy
5. Access Management Policy
6. Information Security Policy

The Policy has been reviewed and discussed at the Policy & Governance Committee meeting of January 12th, 2026.

History

Item:	**Date:**	**Explanation:**
Policy adopted	January 29, 2026	
Annual BOT Review/Reaffirmed		
Previously Reviewed and Extended		
Renamed		

SUNY Erie Cross References

Policy Name or Procedure:	**Where to find:**
Acceptable Use Policy	College Catalog