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

POLICY NAME: Information Security Policy

POLICY TYPE: Managerial

SUBMITTED BY: Daniel Bartkowiak, Information Security Officer

ISSUE OR STATEMENT OF PURPOSE: SUNY Erie Community College ("SUNY Erie" or "the College") is committed to providing accessible, high-quality education while ensuring the confidentiality, integrity, and availability of its information assets.

The Information Security Program Policy (ISP) establishes the framework by which SUNY Erie governs information security. It fulfills SUNY Erie's fiduciary, legal, and regulatory responsibilities under:

- SUNY Policy 6900 (Information Security Policy)
- SUNY Policy 6608 (Campus Programs & Preserving Confidentiality)
- New York State Information Security Breach and Notification Act
- FERPA, GLBA, PCI DSS (where applicable)
- Freedom of Information Law (FOIL)

The Information Security Program Policy is informed by guidance from NIST 800-171 and the Center for Internet Security (CIS) Critical Controls but is tailored to SUNY Erie's role as a community college.

SUNY Erie must establish and implement an information security program (ISP). The ISP must deploy administrative, technical and operation controls to ensure the confidentiality, integrity and availability of the institution's data and systems. The ISP must incorporate an information security risk management process for identifying and responding to information and cyber security threats.

The SUNY Erie Acceptable Use Policy (AUP) forms an integral part of this ISP. The ISP incorporates and enforces user responsibilities, restrictions, and enforcement provisions from the AUP.

NEW OR EDITED POLICY: New

POLICY:

- **Scope:**

  This ISP applies to:

- All information assets owned, managed, or otherwise under the custody or control of SUNY Erie.
- All faculty, staff, students, trustees, contractors, consultants, volunteers, and other authorized users.
- All forms of institutional data: at rest, in transit, and in process.
- All ITS resources, including College-owned devices, College-managed accounts, and personally owned devices connected to College systems where applicable.

Governance:

The Information Security Officer (ISO) is responsible for the oversight and implementation of the Information Security Program (ISP). The ISO is supported by the Director of Information Technology Services.

Definitions:

Authorized Users: All faculty, staff, students, trustees, contractors, volunteers, and affiliates with approved access

Information Security Program (ISP): The framework of policies, procedures, and controls for safeguarding SUNY Erie's information assets.

Acceptable Use Policy (AUP): The companion policy defining individual user responsibilities and restrictions.

Sensitive Data: Personally identifiable information (PII), student records, employee information, health records, financial data, and other regulated or confidential information.

Incident Response Plan: SUNY Erie's formal response framework for information security events (formerly "Data Breach Crisis Plan").

Access Control:

- Accounts remain the property of SUNY Erie and must not be shared without approval.
- In accordance with the Incident Response Plan, ITS reserves the right to restrict accounts and ITS resources.
- Password sharing, impersonation, or unauthorized access attempts are prohibited.
- Access is removed upon separation; accounts are disabled and removed per HR policy.
- Alumni and Emeritus employees do not retain SUNY Erie email accounts.
- ITS reserves the right to audit and modify account permissions to ensure they align with users' job responsibilities and the access required to perform their duties.
- All accounts and Access will be subject to the Access Management Policy

Awareness & Training:

- All users are responsible for using technology effectively and securely.

- ITS will provide cybersecurity awareness training annually and phishing tests throughout the year.
- All Authorized Users are required to complete the annual cyber security awareness training.
- Users with access to sensitive information will receive additional PII data training.

Audit & Accountability:

- ITS may log, monitor, or inspect activity.
- Actions may be taken in consultation with HR, Legal, or the Dean of Students.
- Audits will be conducted periodically following ITS's account audit procedure.
- College correspondence must be conducted through College accounts to ensure FOIL compliance.

Assessment & Authorization:

ITS will assess systems at least annually for risks.

- Develop and implement plans of action designed to correct deficiencies and reduce vulnerabilities in information systems.
- External vendors must undergo risk review and approval by ITS prior to integration.
- Annually assess the security controls in organization information systems to determine if the controls are effective.
- SUNY Erie will comply with the Information Security Risk Management Policy.

AI Usage and Data Governance:

- Use of AI platforms must comply with the AUP.
- Users are strictly prohibited from submitting PII, student records, employee information, or other sensitive College data into non-ITS approved AI tools.

Enforcement & Exceptions:

The College is the sole arbiter of what may constitute a violation of this policy. Violations of this Policy will be adjudicated, as deemed appropriate, and may include the following:

a. Loss of computing privileges

b. Disconnection from the network

c. Disciplinary action

d. Prosecution under applicable civil or criminal laws

All exceptions to Sections 4 through 13 of the SUNY 6900 Information Security Policy must be approved and reviewed annually in accordance with the SUNY Erie's Information Security Exception Procedure.

Exception requests must be approved annually by the Information Security Program lead and the institution's president or the president's designee and retained for record keeping. Exception requests must include the

following information:

- Justification for the exception.
- The anticipated duration of the exception request.
- Compensating controls that are in place to mitigate risks associated with the exception.

Cyber Breach Insurance:
SUNY Erie must obtain insurance for the costs that could result from an information security breach. SUNY Erie must review the Cyber breach coverage annually. Cybersecurity insurance will cover costs that flow from breach discovery, mitigation, and notification, and for the community colleges, liability costs.

SUNY Erie must, to the extent feasible, require third parties who either handle operationally necessary data or provide essential IT services to maintain adequate insurance coverage. This insurance must be sufficient to cover potential losses arising from information security incidents or data breaches, in accordance with New York State law. The requirement applies to third parties integral to the institution's operations or data management, ensuring financial protection in the event of security compromises.

Assessment & Authorization:
This ISP shall be reviewed at least annually by the ISO

A written report, prepared by a qualified individual, assessing the status and effectiveness of the Information Security Program, as well as identifying any material risks, shall be submitted annually to the institution’s executive leadership for review and comment.

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. Security Risk Management Policy

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