Policy:	Information Security Policy	**Policy No.:**	IT9004
Authority:	SUNY Broome Community College Board of Trustees		
Policy Owner:	President	**Responsible Party:**	*Information Technology Services*
Approved:	September 19, 2024		
Revised:	(DATE)		

Purpose

The purpose of this policy is to ensure SUNY Broome Community College (the "College") maintains information and Information Systems in support of the College's educational mission and operations. This Information Security Policy (this "Policy") has been adopted to support protection of the confidentiality, integrity and availability of the College's Information and Information Systems. This Policy also has been adopted to comply with laws governing the College's Information and/or Information Systems.

Statement of the Policy

NIST Cybersecurity Framework

The College will adopt the most current NIST (National Institute of Standards and Technology) Cybersecurity Framework as a tool to achieve cybersecurity outcomes.

Compliance with Applicable Laws and Contractual Obligations

College Information and Information Systems are subject to numerous laws and regulations relating to security. The College also is or may become a party to contracts that require the College to maintain a certain level of information and Information System security. The procedures and guidelines in the Information Security Program shall comply with all applicable legal and contractual requirements governing College Information and Information System security.

Security Program

In order to develop, implement and maintain the Information Security Program in compliance with 16 CFR § 314.4 (see GLBA (Gramm-Leach-Baily Act) reference in Appendix), the College shall:

- Designate a qualified individual responsible for overseeing, implementing and enforcing the Information Security Program.
- Base the Information Security Program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality and integrity of confidential information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.

- Design and implement safeguards to control the risks identified through risk assessment, including:
    - Periodically review access controls, including technical, administrative and physical controls.
    - Identify and manage the data, personnel, devices, systems, and facilities that enable the College to achieve business purposes in accordance with their relative importance to business objectives and the College's risk strategy.
    - Protect by encryption all confidential information held or transmitted by the College both in transit over external networks and at rest.
    - Adopt secure development practices for in-house developed applications utilized for transmitting, accessing, or storing confidential information and procedures for evaluating, assessing, or testing the security of externally developed applications utilized to transmit, access, or store confidential information.
    - Implement multi-factor authentication for any individual accessing any information system, unless the Qualified Individual has approved in writing the use of reasonably equivalent, more, or less secure access controls.
    - Develop, implement, and maintain procedures for the secure disposal of confidential information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and periodically review the College's data retention policy to minimize the unnecessary retention of data.
    - Adopt procedures for change management.
    - Implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, confidential information by such users.
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.
- For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, the College shall conduct:
    - Annual penetration testing of information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

    - Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in information systems based on the risk assessment, at least every six months; and whenever there are material changes to operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on the information security program.
- Implement policies and procedures to ensure that personnel are able to enact the Information Security Program by:
    - Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
    - Utilizing qualified information security personnel to manage the information security risks and to perform or oversee the Information Security Program;
    - Providing information security personnel with security updates and training sufficient to address relevant security risks; and
    - Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.
- Oversee service providers, by:
    - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the confidential information at issue;
    - Requiring service providers by contract to implement and maintain such safeguards; and
    - Periodically assessing service providers based on the risk they present and the continued adequacy of their safeguards.
- Evaluate and adjust the Information Security Program in light of the results of the testing and monitoring required by 16 CFR 314.4(d); any material changes to operations or business arrangements; the results of risk assessments performed under 16 CFR 314.4(b)(2); or any other circumstances that you know or have reason to know may have a material impact on the Information Security Program.
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information. Such incident response plan shall address the following areas:
    - The goals of the incident response plan;
    - The internal processes for responding to a security event;
    - The definition of clear roles, responsibilities, and levels of decision-making authority;
    - External and internal communications and information sharing;
    - Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

    - Documentation and reporting regarding security events and related incident response activities; and
    - The evaluation and revision as necessary of the incident response plan following a security event.
- Require the Qualified Individual to report in writing, regularly and at least annually, to the Board of Trustees. The report shall include the following information:
    - The overall status of the information security program and compliance with this part; and
    - Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.
- Notify the Federal Trade Commission about notification events in accordance with 16 CFR 314.4(j)(1)(2).

Responsibilities and Oversight
The College's Chief Information Officer shall oversee the administration of this Policy and the Information Security Program. The College's Chief Information Officer also shall oversee the training of all users, as set forth in this Policy and the Information Security Program. Subject to approval of the President, the Chief Information Officer may delegate specific functions under this Policy and the Information Security Program, but must retain oversight responsibility.

Reporting of Security Incidents
In the event of a security incident or significant security event, the College's Chief Information Officer or designee and Information Security staff shall report the incident or event to the SUNY CISO, who will then report the incident to the NYS AG in a timely manner compliant with NYS SHIELD Act. Upon discovery of any actual or suspected security incident or significant security event, the Chief Information Officer in coordination with the Information Security staff will determine which, if any, local campus notification requirements apply and shall make such notifications as are required.

Training
All Users of information and Information Systems owned by the College are required to complete annual security awareness training on the appropriate standards for accessing, using and storing information and accessing and using information systems, according to the procedures and guidelines set forth in the Information Security Program. The training program is released the first week of October and will be available until the last day of Summer classes. Completion of annual training during this time frame is a condition of employment.

User Responsibilities
If a User identifies any security issue, suspicious activity, potential security event or incident involving Information or Information Systems, the user must notify the College's Information Technology Security staff immediately. Under no circumstances should the user demonstrate the security issue to another user or encourage any other user to exploit or replicate the security issue. Users also are responsible for protecting and backing up their information regularly using the appropriate College approved and supplied resources.

Relationship to Other Policies and Procedures
Other College policies and procedures may relate to this Policy, including policies and procedures relating to financial, educational and human resources information. In the event of any variance between or among the College's policies and procedures, the College will follow the most protective standard governing the security of such information.

Enforcement
Violations of this Policy or the Information Security Program may result in suspension or loss of a user's privileges to access or use Information or Information Systems, based on the guidelines set forth in the Information Security Program and/or pursuant to other applicable College policies and procedures. Additional penalties also may apply pursuant to other College policies, contracts, and/or applicable civil and criminal laws.

To Whom It Applies (title or department)
This policy applies to all students, faculty, affiliates, emeriti, and staff of the College (part-time and full-time), as well as all independent contractors, interns, consultants, and other third parties, inclusive of anyone who has access to network or email services. The policy applies regardless of the user's physical location (e.g., College offices, hotels, airports, user homes, etc.).

Definitions
For the purpose of this policy, the following definitions apply:
"Affiliate" is defined as the Foundation, FSA, and Housing Development Corporation.

"College Technology Resources" is defined as all computers, wired and wireless networking equipment, portable electronic devices, interactive white boards, projectors, and other electronic devices used to support the College's educational mission and operational functions. The term College Technology Resources includes all Information Systems, as defined below.

"Information" is defined as any information that is owned or licensed by the College, or is stored, processed or transmitted on any College Information System.

"Information System" is defined as any electronic system owned or licensed by the College that stores, processes or transmits Information.

“Information Security Program" is defined as the procedures and guidelines for implementing this Policy.

“Personally Identifiable Information” (PII) is defined as any information relating to an identified or identifiable natural person.

“Security Incident” is defined as any actual or suspected event affecting the confidentiality, integrity or availability of Information or any Information System.

“User” is any individual member of the College Community who interacts with SUNY Broome information systems or College technology resources.

Appendix
NIST CyberSecurity Framework 2.0
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NYS SHIELD Act
https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

GLBA
Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements | Knowledge Center

Action *(Created, Reviewed, Retired)*	**Date**	**Initials**	**Position Title**
Created	08/02/2024	BAM	*Chief Information Officer*