SUNY SCHENECTADY COUNTY COMMUNITY COLLEGE

Facilities

Board of Trustees Policy

SUBJECT:	NUMBER:
Information Security Policy	**5.5**
	DATE: **November 20, 2023** **Resolution # 23-141**
	SUPERSEDES: **March 19, 2018** **Resolution # 18-32**

Purpose

SUNY Schenectady (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.

This Policy applies to all students, faculty, staff, contractors and others ("Users") duly approved to access the College's Information and/or Information Systems, pursuant to the College's policies and procedures relating to use of College Technology Resources.

Definitions

"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" 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.

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.

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 Office 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

The Chief Information Officer shall report to the Office of the President promptly in the event of any Security Incident, based on the procedures and guidelines set forth in the Information Security Program.

The Office of the President shall notify the Board of Trustees promptly in the event of any Security Incident that (a) affects personally identifiable information of any person or financial information of the College or (b) creates a material risk of harm to the College or

its operations.

Depending on the nature and severity of the Security Incident, the College also may be required to make certain notifications pursuant to applicable laws, regulations or contractual agreements. Upon discovery of any actual or suspected Security Incident, the College will determine which, if any, notification requirements apply and shall make such notifications as are required.

Training

All Users of Information and Information Systems are required to receive 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.

College Liability and User Responsibilities

No security controls are one hundred percent (100%) effective to eliminate all threats. The College is not responsible for the failure of any security controls to preserve the confidentiality, integrity or availability of Information transmitted, used or stored on Information Systems. The College is not responsible for the failure of any security controls to preserve the confidentiality, integrity or availability of any Information System.

If a User identifies a security issue involving Information or Information Systems, the User must notify the College's Information Technology 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.

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.

Adoption and Update of the Information Security Program

To ensure compliance with this Policy, the Office of the President, the Chief Information Officer and such other persons as the Office of the President deems necessary, shall review and update all current Information and Information System security policies and procedures and prepare a new Information Security Program by June 30, 2018.

At least annually thereafter, the Office of the President, the Chief Information Officer and such other persons as the Office of the President deems necessary shall review and update the Information Security Program to reflect changes in the College's Information and Information Systems, changes in technology, changes in applicable law and any other factors affecting the confidentiality, integrity and availability of the College's Information and Information Systems.