SUNY SCHENECTADY COUNTY COMMUNITY COLLEGE

Facilities

Board of Trustees Policy

SUBJECT:	NUMBER:
Information Security Incident Investigation, Response, and Notification Policy	**5.4**
	DATE: **November 20, 2023** **Resolution 23-140**
	SUPERSEDES: **June 18, 2018** **(Resolution # 18-84)**

Purpose

The College maintains Information – including personal information of students, faculty and staff – that may be disclosed due to inadvertent actions, cyberattack, or other unplanned events (collectively, "Security Incidents"). Pursuant to law, regulation and certain contracts, the College is required to investigate, respond to and provide notice of certain Security Incidents to affected individuals, government authorities, and other interested parties. This Policy authorizes the College's administration to take appropriate steps to comply with the College's Security Incident investigation, response and notification obligations.

Policy

The SUNY Schenectady County Community College (the "College") will investigate, respond to, and provide required notices of information security incidents to affected individuals, government authorities, and other interested parties

Compliance with Applicable Laws, Contracts, and Industry Best Practices and Standards
Many laws contain Security Incident investigation, response and notification requirements, including but not necessarily limited to: (1) New York State Technology Law § 208, (2) the Gramm-Leach-Bliley Act ("GLBA") and related regulations, and (3) the Health Insurance Portability and Accountability Act ("HIPAA"), and (4) the General Data Protection Regulation ("GDPR"). From time-to-time the College enters into the

federal financial aid program. In addition, from time-to-time, the College may deem it advisable and/or necessary to provide notices of other Security Incidents pursuant to industry best practices and standards.
The definition of covered information, scope of notification requirements and procedures for notification vary. Consistent with the requirements of Policy No. 4.15, each Security Incident

must be examined independently to determine whether the Security Incident affects Information covered by any applicable law, regulation or contract.

The College shall follow all legal and contractual requirements. The College's Information Security Program may also include procedures that the Chief Information Officer deems advisable, including industry best practices and standards. contracts that include notification requirements, including but not limited to contracts relating to:

Relation to Other Policies

This Policy is related to the College's Information Security Policy (No. 5.5). All capitalized terms in this Policy have the same meaning as those terms in Policy No. 5.5.

Procedures

Security Incident Response Team

To ensure timely investigation, response and notification, the College will form and maintain a Security Incident Response Team ("SIRT") to respond to any Security Incident. The College's Chief Information Officer is a permanent member of the SIRT. The Office of the President is directed to appoint additional members to the SIRT based on the requirements of the College's Information Security Program. The roles and responsibilities of the SIRT will be set forth and updated from time-to-time in the College's Information Security Program

Investigation, Response and Notification of Security Incidents

Consistent with Policy No. 5.5, all Security Incidents must be reported to the College's President, even if such Security Incident does not require further notification to any third parties. As also set forth in Policy No. 5.5In the event of a Security Incident, the College will determine which, if any, additional notification requirements apply and shall make such notifications as are required or the College deems to be advisable under the circumstances. The College's Information Security Program shall include detailed procedures for investigating, responding to, and providing notices in the event of a Security Incident. To streamline and ensure timely compliance, the College's Information Security Program shall also include defined procedures for notification of specific types of breaches (e.g., breaches of personal information covered under New York State Technology Law § 208 and breaches of covered financial aid information under applicable federal laws and regulations). No notification may be made without the prior approval of the College's President, the Chairperson of the Board of Trustees, or such other person specifically authorized by the College's President and/or the Chairperson of the Board of Trustees.

Responsibilities and Oversight

The College's Chief Information Office shall oversee the administration of this Policy. Subject to approval of the Office of the President, the Chief Information officer may delegate specific functions under the Policy, but must retain oversight responsibility.

Approved by the SUNY Schenectady Board of Trustees, November 20, 2023, Resolution # 23-140 Information Security Incident Investigation, Response, and Notification Policy.