Category: Information Security Legal and Compliance Responsible Office: Chief Information Officer	Policy Title: Information Security Policy Document Number: 6900 Effective Date: September 14, 2016 This policy item applies to: Community Colleges State-Operated Campuses Statutory Colleges System Administration

Table of Contents

Summary

Responsible System Office: Chief Information Officer

Responsible Campus Office: Campus President

The State University of New York ("SUNY" or "State University") is committed to securing and protecting the information within its possession. As an institution of higher education operating in New York State, SUNY must comply with federal and state confidentiality and information safeguarding laws, as well as meet data protection requirements imposed by its accrediting agency, the Middle States Commission on Higher Education ("MSCHE"). SUNY's core academic mission and strategic goals require policies, procedures, controls, monitoring and verifications to protect the information it possesses or transmits through the normal course of operations. In an increasingly digital environment, the broad range of information central to the facilitation of academic programs, student services, and overall business operations in the State University's possession has made such information one of SUNY's most important assets, requiring increased vigilance with respect to storing, sharing, and using data that builds on existing SUNY policy and practice.

The scope of SUNY's academic programs and mission requires secure information sharing between its State-operated campuses, statutory colleges, and community colleges as well as with System Administration, for the facilitation of academic programs and student services, ongoing improvement, and oversight.

SUNY's policies on assessment and institutional effectiveness including, most recently, the Data Transparency and Reporting Policy adopted by the SUNY Board of Trustees in 2013 (Resolution No. 2013-025) affirmed principles for data integrity and use of data to strengthen and report on progress of the academic programs at each institution. The Data Transparency and Reporting Policy directed each SUNY campus to develop and implement plans for the regular

assessment and review of programs. Such plans are to contain elements to preserve and protect data, not only for the purpose of addressing confidentiality concerns, but also to ensure integrity and accuracy in reporting for program quality and success in meeting and exceeding applicable standards placed upon SUNY by state and federal law, the New York State Education Department, and MSCHE.

Finally, the legal and reputational risks involved in the potential breach of security of data require campuses to evaluate the need to pursue insurance to protect against loss in the event of a security breach which can result not only from legal fees, but also the losses that go beyond litigation, including breach incident response costs, breach notification procedures, mitigation measures to protect those whose information was affected, crisis management teams, and damage to the institution's reputation.

In order to obtain breach insurance coverage, campuses are required to verify that they have, and comply with, a robust information security policy. For these reasons, it is imperative for SUNY to maintain a system-wide Information Security Policy.

Policy

Purpose

The objective of this policy is to ensure that the State University's information assets, including academic, health, research, financial, and other information deemed non-public, are adequately safeguarded. It is the responsibility of the State University to ensure the confidentiality of its non-public information, while preserving the integrity and availability of the public information that is stored, processed, and/or transmitted on SUNY's campuses and System Administration. Additionally, the State University must be diligent in its efforts to protect the academic, research, financial, health and personal information of its faculty, staff, students, and all persons interacting with SUNY's institutions. This policy will help protect SUNY's information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. Furthermore, this policy clarifies the responsibility of SUNY campuses and System Administration regarding existing security policies and procedures. All members of the State University community and users of SUNY data are expected to adhere to this policy and take the necessary measures to protect and secure data they possess and transmit.

Accountability

The Information Security Policy is a SUNY system-wide policy that applies to:

- Authorized users at System Administration, State-operated campuses, and community colleges;
- Statutory Colleges with respect to sharing of information with SUNY campuses and System Administration;
- Entities, affiliates, and third-party service providers that rely upon the State University's data for their operations and/or service delivery;
- Any users of System Administration, State-operated campuses, and community colleges services and data; and
- All SUNY information and records, where records are documentary material, in any format, both digital/electronic or physical hard copy documents, that are transmitted or stored by a campus or System Administration, and have a legal, operational, or historical value to the institution.

In accordance with this policy, campuses and System Administration are responsible for:

- Implementing an Information Security Program in accordance with this policy, and other related SUNY policies and procedures; and
- Following appropriate security protocols as outlined in this policy, related policies, and applicable standards, guidelines and procedures to protect data that is in their possession.

Requirements

A. The Information Security policy mandates that SUNY institutions:

- Adhere to SUNY policies, procedures, and state law regarding information assets and systems—which are to be incorporated into this policy and forthcoming procedure—specifically:
  - Records Retention and Disposition SUNY Policy and State Schedules:
    - SUNY Policy Document No. 6609 - Records Retention and Disposition Policy- applicable to State-operated campuses.
    - New York State General Retention and Disposition Schedule for New York State Government Records- applicable to State-operated campuses.
    - MI-1 State Records Retention and Disposition Schedule – applicable to community colleges.
    - CO-2 State Records Retention and Disposition Schedule – applicable to community colleges.
  - SUNY Policy Document No. 1100 – Data Transparency and Reporting - applicable to State-operated campuses, community colleges, and statutory colleges.
  - SUNY Procedure Document No. 6608 - Information Security Guidelines: Campus Programs & Preserving Confidentiality –applicable to State-operated campuses, community colleges, and statutory colleges.
  - SUNY Procedure Document No. 6610 - Legal Proceeding Preparation (E-Discovery) Procedure – applicable to State-operated campuses.
  - SUNY Procedure Document No. 6601- Compliance with Freedom of Information Law (FOIL)- applicable to State-operated campuses, community college campuses, and statutory colleges;
- Designate an Information Security Officer (ISO);
- Develop an incident response process to ensure timely notification to campus leadership, including the campus President, of cyber security incidents and information security breaches involving exposure of regulated or personally identifiable data;
- Ensure timely immediate notification to System Administration officials in the event of a critical suspected or actual information breach or cybersecurity incident, as is set forth in the existing System Administration Incident Response process;
- Complete the annual Self-Assessment Questionnaire disseminated by System Administration's Chief ISO;
- Ensure encryption of State University information and information systems, as appropriate;
- Provide annual training to all individuals who access State University information assets and systems;
- Adopt local campus policies regarding information security;
- Require that any third parties who will store data, both paper and electronic, on behalf of SUNY, have insurance in place to cover losses in the event of an information security or breach incident consistent with New York State law;
- Continually assess and monitor vulnerability of information security. This policy encourages campus participation in the SUNY Security Operations Center (SOC) to help with this assessment and monitoring; and
- Obtain breach insurance for the costs that result from an information security breach consistent with SUNY guidelines that will be set forth in detail in the implementing procedures to this policy. Generally, breach insurance will cover costs that flow from breach discovery, mitigation, and notification, and for the community colleges, liability costs. For State-operated campuses, liability costs are generally covered by the Court of Claims fund.

B. With respect to SUNY's statutory colleges, the Information Security policy mandates that statutory colleges certify that they have in place the above-referenced elements or similar measures, which have been deemed by SUNY System Administration to offer the equivalent protections.

Definitions

There are no definitions relevant to this policy.

Other Related Information

Records Schedules governing retention and disposition of information at SUNY campuses:

- State-operated campuses:
  - SUNY Records Retention and Disposition Policy 6609 (listed in the appendices to the SUNY Records Policy)
  - New York State General Retention and Disposition Schedule for New York State Government Records
- Community Colleges:
  - MI-1 Records schedule (for all miscellaneous governments) followed by Adirondack, Columbia-Greene, Corning, Fulton-Montgomery, Jamestown, North Country and Tompkins-Cortland Community Colleges and the Fashion Institute of Technology
  - CO-2 Records schedule (for county governments) should be followed by all other Community Colleges

Federal Educational Rights and Privacy Act (FERPA) - Information available on the SUNY Compliance FERPA webpage

Health Insurance Portability and Accountability Act (HIPAA) - Information available on the SUNY Compliance HIPAA webpage

Gramm- Leach- Bliley Act - Information available on the SUNY Compliance GLBA webpage

Payment Card Industry Data Security Standard (PCI DSS)

NYS Information Security Breach & Notification Law

NYS Business Law and Technology Law

NYS Governmental Accountability, Audit & Internal Control Act

NYS Information Security Policy P03-003

NYS Education Law, including, but not limited to, §6304(12), relating to electronic transactions at the community colleges

Community Rights & Responsibilities

Procedures

SUNY Procedure Document No. 6608 - Information Security Guidelines: Campus Programs & Preserving Confidentiality

SUNY Procedure Document No. 6610 - Legal Proceeding Preparation (E-Discovery) Procedure

SUNY Document No. 6601 - Compliance with Freedom of Information Law (FOIL).

Related Policies

SUNY Policy Document No. 6609 - Records Retention and Disposition Policy, with Introduction to the SUNY Records Retention and Disposition Schedule.

SUNY Data Transparency Policy.

Forms

There are no forms relevant to this policy.

Authority

State University of New York Board of Trustee Resolution, No. 2016-51.

NYS Education Law §351, NY EDN Title 1, Article 8, §351 (State University Mission).

In case of questions, readers are advised to refer to the New York State Legislature site for the menu of the Laws of New York State.

History

September 14, 2016, Board of Trustee Resolution No. 2016-51, Information Security Policy.

Appendices

There are no appendices relevant to this policy.