Category: Information Security Legal and Compliance Responsible Office: University Counsel	Procedure Title: Information Security Guidelines: Campus Programs & Preserving Confidentiality Document Number: 6608 Effective Date: February 01, 2008 This procedure item applies to: Community Colleges State-Operated Campuses Statutory Colleges

Table of Contents

Summary

Pursuant to federal and state laws and University policy and procedures governing internal controls and the protection of certain categories of information applicable to the business of State University of New York, this procedure provides guidelines for the campus information security program. The procedure's 13 standards define the program's structures and functions and require the program be used, at a minimum, to protect the confidentiality of legally defined categories of sensitive information and such information's related systems for storage, retrieval, processing, transmission and security.

Process

This Procedure presents the fundamental standards of action required of Campuses to:

- establish the fundamental campus structures and functions needed to conduct a legally and professionally sound Program that applies risk management appropriately to all information and system assets;
- engage the Program effectively and immediately in protecting the confidentiality (appropriate use and disclosure) of Sensitive Information and the operational integrity of Sensitive Systems; and
- begin incorporating into the Program the two other major categories of information security, which are preserving the integrity (intended content) and availability (intended operational access) of Sensitive Information and Sensitive Systems.

The standards cover the fundamental categories of risk management, outlined as follows:

A. Establish Program Organization

A1. Responsible, Authorized Experts
A2. Executive Oversight
A3. Comprehensive Scope
A4. Documentation and Compliance Reporting

B. Declare Campus Policy and Standards

B1. Declaration of Sensitive Categories
B2. Campus Policy and Standards

C. Create and Maintain Risk-Oriented Inventories

C1. Asset Inventory
C2. Workforce Inventory

D. Conduct Analysis of Risk, Practices, and Protections

D1. Risk Analysis
D2. Analysis of Practices and Protections

E. Improve and Maintain Practices and Protections

E1. Improved Practices and Protections
E2. Learning
E3. Readiness

A. Establish Program Organization

A1. <u>Responsible, Authorized Experts</u>

Campus executive management names, authorizes, and requires at least one person to:

- understand the campus's information security risk;
- understand the Program and the meaning and intent of the Standards;
- present professionally and legally sound and timely advice to executive management regarding appropriate action; and
- ensure the Program is exposed to outside, professional perspective, especially that of the University's central information security oversight function.

The traditional form for this role is the Information Security Officer ("ISO"). If circumstances do not allow for a dedicated position for this function, the "ISO" role may be handled by an assigned, organized set of people and might then be called Information Security Oversight (or Office). The amount of time and energy dedicated by the "ISO" matches the size, complexity, and type of mission of the campus. The University's HIPAA-covered SUNY Campuses (see Definitions) must, by law, designate a single individual as having overall, final responsibility for the security of the entity's electronic healthcare information.

References: , 5.1(c); , 6.1.3, 6.1.7; , Part 2, p.6; 314.4(a); 164.308(a)(2), and sections 8377 and 8347-48.

A2. Executive Oversight

At least one executive ("Senior Executive") with power to commit institutional funds and personnel:

- approves the Program;
- oversees the Program's implementation;
- ensures individual managers are assigned ownership and stewardship responsibilities for critical information assets and are given adequate time and resources; and
- responds on behalf of the campus to the advice received from the "ISO."

References: , 7; , 6.1.1; , Part 4, p.10; III(A) and (F).

A3. Comprehensive Scope

The "ISO" collaborates actively with (or if the "ISO" is a team, it consists of) key managers of the major business functions of the campus ("Colleagues") to ensure that:

- the "Colleagues" participate at least in the major risk decisions regarding information for which they are owners or designated as responsible;
- all elements of the Program are coordinated; and
- each subsidiary of the campus participates in the Program in appropriate ways.

References: , 4.2.1(a), 5.2.1(b); , 6.1.2; , Part 2(C); II(A).

A4. Documentation and Compliance Reporting

The "Senior Executive" and "ISO" keep professionally and legally sound documentation of their key actions and decisions. They also authorize and require the creation and use of other forms of strategic and operational documentation ("Program Documents") and include these in their declarations of "Sensitive Information." "Program Documents" include the text that formally authorizes the Program ("Program Authorization") and a plan ("Program Documentation Plan") describing the owners, storage locations, completion date, and subject of each "Program Document." The documentation plan includes at least the documents shown below, which are the critical records and reports arising from the actions required by the Standards in this Procedure. Any of these documents may in practice be with similar content, purpose, and format. Each document collects and presents some of the work done in service of one of the Standards, as indicated in the table below. But each document also serves the work of at least one other Standard. Campuses determine the precise content, formatting, and names for their "Program Documents." See Appendix B, for further guidance.

Program Organization (Standards A1-A4)

1.
2.

Policy & Standards (Standards B1, B2)

3.
4.

Inventory (Standards C1, C2)

5.
6.

Analysis (Standards D1, D2)

7.
8.
9.

Practices & Protections (Standards E1, E2)

10.
11.
12.

The Campus delivers at least annually to System Administration's office for information security oversight ("OISO") the "Program Documentation Plan" and the "Summary of Project Plans and Outcomes." It also delivers any other documents the "OISO" requests in support of its mission to assure or determine levels of compliance with the Procedure and the ongoing development of the Program. The Campus should review the Plan and make any necessary updates on a regular basis, at least every other year.

References: , 4.3.1; , 5.1.2, 6.1.3; , throughout; 164.316(b).

B. Declare Campus Policy and Standards

B1. <u>Declaration of Sensitive Categories</u>

The "Senior Executive" authorizes and communicates to appropriate members of the campus community the campus categorization and classification of sensitive information ("Sensitive Information") assets, regardless of format, and the systems ("Sensitive Systems") related to sheltering, storing, processing, and transmitting of the "Sensitive Information," including all such categories covered by law and all categories defined by the University's management. These categories include (see Appendix C):

- the "Program Documents;"
- student education records as defined in FERPA;
- personal information as defined in the NYS Personal Privacy Protection Law;
- health information as defined in HIPAA;
- customer information defined in GLBA; and
- personal identifying information as defined in NYS Business Law and Technology Law for breach notification and records disposal.

The "Senior Executive" also communicates to the Campus the principles and rules for using "Sensitive Information" and for assigning roles for such use to members of the campus community and external parties.

References: , 4.2.1(d)(1); , 7.13, 7.2, 8.1.1; , Part 5(A), p.11; many categories are defined in law, e.g., , , , .

B2. <u>Campus Policy and Standards</u>

The "Senior Executive" authorizes and communicates to appropriate members of the campus community the security

policy and standards to which it expects adherence, at least with respect to:

- relevant laws and regulations;
- the confidentiality of "Sensitive Information;"
- managing campus information risk through a legally and professionally sound program; and
- specifying responsibilities, including managers' ownership and stewardship of critical information assets and related systems.

References: , 4.2.1(b), 5.1(a,b,d); , 5.1, 15.1; , 4, p.10; 164.316(a); (12); many standards are law, e.g., , , , _ t.

C. Create and Maintain Risk-Oriented Inventories

C1. <u>Asset Inventory</u>

The campus maintains at least one inventory ("Asset Inventory") of the most critical forms of "Sensitive Information" and "Sensitive Systems." The "Asset Inventory" presents the essential facts needed by the "ISO" and "Colleagues" to analyze the risks to the confidentiality, integrity, and availability of those assets and includes asset type, location, owner, users, custodians, business value, sensitivity, and backup information.

References: , 4.2.1(d)(1); , 7.1.1; , Part 5, p.25.

C2. <u>Workforce Inventory</u>

The campus maintains at least one inventory ("Workforce Inventory") of workers with authorized access to the objects in its "Asset Inventory." The "Workforce Inventory" presents the essential facts needed by the "ISO" and "Colleagues" to analyze the security risks to those assets and includes work location, work group and supervisor, security roles and object authorizations.

References: , 4.2.1(d)(1); , 11.2; Part 10; III(C)(1)(a).

D. Conduct Analysis of Risk, Practices, and Protections

D1. <u>Risk Analysis</u>

At least annually, the "ISO" conducts or oversees a professionally and legally sound analysis ("Risk Analysis") at least of the risk to the confidentiality of the "Sensitive Information" in the "Asset Inventory." The "Risk Analysis":

- considers foreseeable threats and hazards that could result in substantial harm or inconvenience to the University or to persons who are the subject of the personal information in the "Asset Inventory."
- attempts to identify the most important remaining risk, taking into account:

  a. the protections already in place; and
  b. the skills and vulnerabilities associated with the persons in the "Workforce Inventory."

The "Risk Analysis" looks for well-known threats with high likelihood and impact, but also attempts to expand the depth and scope of what has previously been known.

References: , 4.2.1(c,d,e); , 4; , Parts 5,8,9,10,11; III(B); 164.308 (a)(1)(ii) (A); (RA).

D2. Analysis of Practices and Protections

The “ISO” maintains an ongoing, professionally and legally sound analysis (“Analysis of Practices and Protections”) of required, existing, and missing practices and protections that mitigate or otherwise address the risks identified in the “Risk Analysis.” The “Analysis of Practices and Protections” generates or updates a campus-specific “Catalog of Practices and Protections,” or several such Catalogs relating to specific domains of responsibility and/or specific types of information and information systems. The Catalogs’ items are not broad categories, such as those given below, but are concise descriptions of identifiable practices (e.g., using hard-to-guess passwords) and protections (e.g., laptop encryption, anti-virus, door locks). The items are sufficiently detailed to enable managers, the general workforce, faculty, and students to identify and work effectively with the instances of each item in their domains, including enriching the entries with local specifics regarding locations, product names and versions, and responsible operators. The sample entries in Appendix E exemplify this.

The “Analysis of Practices and Protections” notes whether each item in the Catalog(s) is:

- a well-known professional standard of good practice;
- required by prevailing law and regulation;
- already in place, including where;
- missing, yet important, reasonable, and appropriate for the campus.

In subsequent rounds of analysis, if not at the first, the analysis reports the extent to which existing practices and protections are effective.

In conducting the analysis and building the “Catalog of Practices and Protection,” the “ISO” includes, at a minimum, the following well-known categories that address the confidentiality of the information:

-
-
-

-
-

-
-
-
-

Forms

There are no forms relevant to this procedure.

Related Procedures

Internal Control Program Guidelines, Document #7501 - Internal Control Program Guidelines

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

Related Policies

SUNY Policy, Records Retention and Disposition, Policy Document No. 6609

Introduction to the SUNY Records Retention and Disposition Schedule, Policy Document Number 6609 Appendices

Other Related Information

Records Retention and Disposition at SUNY Campuses Guidance

Authority

Law:

NYS Personal Privacy Protection Act (PPPL), and University Compliance: Document #6603.

A. Obligations of the University

1.(g) establish written policies in accordance with law governing the responsibilities of persons pertaining to their involvement in the design, development, operation or maintenance of any system of records [collection or grouping of personal information about a data subject, with exceptions], and instruct each such person with respect to such policies and the requirements of the PPPL, including any other rules and regulations and procedures adopted pursuant to the PPPL and the penalties for noncompliance; (h) establish appropriate administrative, technical and physical safeguards to ensure the security of records.

Federal Family Educational Rights and Privacy Act (FERPA)

NYS Freedom of Information Act (FOIL)

NYS Governmental Accountability, Audit and Internal Control Act

Federal Health Insurance Portability and Accountability Act (HIPAA)

Federal Gramm-Leach-Bliley Act (GLBA) and Federal Trade Commission Safeguards Rule

NYS Information Security Breach and Notification Act

NYS Disposal of Personal Records Law

University Compliance Policy:

Use of Social Security Numbers, Document #6604

NYS Freedom of Information Act (FOIL), Document #6601

Family Educational Rights and Privacy Act, Compliance with, Document #6600

Internal Control Program, Document #7500

Health Insurance Portability and Accountability Act, Document #4200

Memorandum to University presidents by University Counsel regarding Gramm-Leach-Bliley Act

State Policy:

NYS Information Security Policy, P03-001 and P03-002; related Standards

NYS

Industry Standards:

Payment Card Industry Data Security Standard (PCI-DSS)

ISO 27001 and ISO 27002

History

Procedure established February 1, 2008.

Appendices

Information Security Guidelines - Appendix C: Declaration of Sensitive Information

Information Security Guidelines - Appendix D: History of Related Legal Requirements

Information Security Guidelines - Appendix A: References

Information Security Guidelines - Appendix F: Confidentiality Practices & Protections in New York State

Information Security Guidelines - Appendix G: Information Security Practices Recommended by New York State

Information Security Guidelines - Appendix B: Program Documents

Information Security Guidelines - Appendix H: Information Security Practices Recommended by New York State