Category: Legal and Compliance Responsible Office: Administrative Services and Technology	Procedure Title: Information Security Guidelines, Part 1 Campus Programs & Preserving Confidentiality Document Number: 6608 Effective Date: February 1, 2008 This procedure item applies to: State-Operated Campuses

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. Responsible, Authorized Experts

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: ►*ISO 27001*, 5.1(c); ►*ISO 27002*, 6.1.3, 6.1.7; ►*NYS P03-002*, Part 2, p.6; ►*GLBA* 314.4(a); ►*HIPAA* 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: ►*ISO 27001*, 7; ►*ISO 27002*, 6.1.1; ►*NYS P03-002*, Part 4, p.10; ►*GLBA IG* 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: ►*ISO 27001*, 4.2.1(a), 5.2.1(b); ►*ISO 27002*, 6.1.2; ►*NYS P03-002*, Part 2(C); ►*GLBA IG* 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 *a designed, controlled set of like documents* 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, *Program Documents* for further guidance.

Program Organization (Standards A1-A4)

1. *Program Authorization*
2. *Program Documentation Plan*

Policy & Standards (Standards B1, B2)

3. *Sensitive Information Categories*
4. *Policy and Standards*

Inventory (Standards C1, C2)

5. *Asset Inventory*
6. *Workforce Inventory*

Analysis (Standards D1, D2)

7. *Risk Analysis*
8. *Catalog of Practices and Protections*
9. *Analysis of Practices and Protections*

Practices & Protections (Standards E1, E2)

10. *Summary of Project Plans and Outcomes*
11. *Training & Awareness Plan and Record*
12. *Incident Response Plan*

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: ►*ISO 27001*, 4.3.1; ►*ISO 27002*, 5.1.2, 6.1.3; *NYS P03-002*, throughout; ►*HIPAA* 164.316(b).

B. Declare Campus Policy and Standards

B1. Declaration of Sensitive Categories

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: ►*ISO 27001*, 4.2.1(d)(1); ►*ISO 27002*, 7.13, 7.2, 8.1.1;►*NYS P03-002*, Part 5(A), p.11; ►many categories are defined in law, e.g., *FERPA*, *GLBA*, *HIPAA*, *NYS Personal Privacy Protection Act*.

B2. Campus Policy and Standards

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: ►*ISO 27001*, 4.2.1(b), 5.1(a,b,d); ►*ISO 27002*, 5.1, 15.1; ►*NYS P03-002*, 4, p.10; ►*HIPAA* 164.316(a); ►*PCI* (12); ►many standards are law, e.g., *FERPA*, *GLBA*, *HIPAA*, *NYS Personal Privacy Protection Act*.

C. Create and Maintain Risk-Oriented Inventories

C1. Asset Inventory

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: ►*ISO 27001*, 4.2.1(d)(1); ►*ISO 27002*, 7.1.1; ►*NYS P03-002*, Part 5, p.25.

C2. Workforce Inventory

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: ► *ISO 27001*, 4.2.1(d)(1); ►*ISO 27002*, 11.2; ►*NYS P03-002* Part 10; ►*GLBA IG* III(C)(1)(a).

D. Conduct Analysis of Risk, Practices, and Protections

D1. Risk Analysis

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: ►*ISO 27001*, 4.2.1(c,d,e); ►*ISO 27002*, 4; ►*NYS P03-002*, Parts 5,8,9,10,11; ►*GLBA IG* III(B); ►*HIPAA* 164.308 (a)(1)(ii) (A); ►*FIPS 200* (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:

a. **ARCHITECTURE, CONFIGURATION**: practices and protections that maintain industry-standard security architecture, principles, and configuration settings in the "Sensitive Systems," which are physical and digital containers of "Sensitive Information," especially the buildings, rooms, computers, networks, databases, and applications that process, store, and transmit "Sensitive Information;"

b. **NETWORK**: protections that control information transmitted or received at the external boundaries and key internal boundaries of "Sensitive Systems;"

c. **TRAINING**: practices that engage the workforce in understanding, assessing, and addressing risk to "Sensitive Information" and "Sensitive Systems;"

d. **SCREENING**: practices that screen potential workers who would be in a position that handles "Sensitive Information" and "Sensitive Systems;"

e. **CONTRACTS**: practices that monitor third parties that handle "Sensitive Information" and "Sensitive Systems" or contractually require them to adhere to standards of good practice;

f. **ACCESS, IDENTITY, AUTHORIZATION**: practices and protections that limit only to authorized persons and processes the access to "Sensitive Information" and "Sensitive Systems" and limit such access only to authorized transactions and functions;

g. **MINIMUMS, NEED-TO-KNOW**: practices that keep to a minimum, based on business need, the types and instances of "Sensitive Information" used in the business processes and the persons and processes authorized to access it;

h. **ACCIDENTS, INATTENTION**: practices and protections that reduce the threat of accidental disclosure of "Sensitive Information" through authorized mechanisms, such as websites, computer terminals, paper printouts, remote access, electronic commerce, online transactions, portable storage devices (laptops, USB flash, PDA, cell phones, etc.,) and the disposal of storage media;

i. **MISCONDUCT**: practices and protections that reduce the threat of employees and contracted external parties illegally or improperly disclosing "Sensitive Information," especially to unauthorized persons seeking the information through fraudulent means;

j. **SYSTEM VULNERABILITY**: protections that reduce the threat of information theft through exploitation of vulnerabilities in computer systems and applications, especially in systems developed in-house and systems connected to the Internet;

k. **ENCRYPTION**: protections that encrypt and otherwise mask electronic data containing "Sensitive Information;"

l. **DETECTION**: practices and protections that detect attacks and intrusions to "Sensitive Information" and "Sensitive Systems" and record and trace actions sufficiently to hold individual actors accountable;

m. **INCIDENTS**: practices that enable workers to respond quickly, appropriately, and with skill when intrusions to "Sensitive Systems" and unauthorized disclosures or leaks of "Sensitive Information" occur.

References: ►*ISO 27001*, 4.2.2; ►*ISO 27002* throughout; ►*NYS P03-003* throughout; ►*GLBA IG* III(C); ►*HIPAA* 164.308(a)(1)(ii)(B); ►*FIPS 200* (AC, AT, CA, CM, IA, MP, PE, PS, RA, SC, SI; ►*PCI* throughout.

E. Improve and Maintain Practices and Protections

E1. Improved Practices and Protections

The "ISO" and "Colleagues" make ongoing, principled, prioritized, documented decisions and proposals to improve the campus's practices and protections, at least with respect to "Sensitive Information" and "Sensitive Systems." These decisions and proposals address the findings of their "Risk Analysis" and "Analysis of Practices and Protections" and generate modifications to the "Catalog of Practices and Protection." The "ISO" and "Colleagues" oversee the design and implementation of projects that implement the changes they advocate, maintain an ongoing "Summary of Project Plans and Outcomes," and assess the effectiveness of these projects in their ongoing "Risk Analysis."

References: ► *ISO 27001*, 4.2.4, 7.1, 8.1, 8.3; ►*ISO 27002* 6.1.2; ►*NYS P03-002*, Part 4; ►*GLBA IG* III(B)(3); ►*HIPAA* 164.308(a)(1)(ii)(B); ►*FIPS 200*; ►PCI.

E2. Learning

Members of the campus community, at least those in the "Workforce Inventory," spend appropriate amounts of time and attention:

- understanding the campus policy, standards, practices, and protections that relate to their work and activities;
- addressing the risks associated with their work and activities, at least with respect to the confidentiality of "Sensitive Information;" and
- learning skills required to apply the security practices and protections required by their work and activities.

References: ►*ISO 27001*, 5.2.2; ►*ISO 27002*, 8.2.2; ►*NYS P03-002* Part 6, p.12; ►*GLBA IG* III(C)2; ►*HIPAA* 164.308(a)(5)(i); ►*FIPS 200*; ►*PCI* (12).

E3. Readiness

The "Senior Executive," "ISO," and "Colleagues" maintain an "Incident Response Team" that includes representatives from Legal, IT, Public Relations, and Law Enforcement and that maintains plans and procedures that enable them to:

- receive timely—which sometimes means immediate—reports of incidents; and

- respond quickly and according to law to security incidents,
  a. especially to breaches of confidentiality in "Sensitive Information;" and
  b. specifically to the breaches of Personal Identifying Information defined in the NYS Information Security Breach and Notification Law; and
  c. assessing the potential damage, coordinating containment and law enforcement activities, and disseminating information regarding the incident to appropriate persons and entities (e.g., potential victims, press, and authorities).

References: ►*ISO 27001*, 4.2.2(h); ►*ISO 27002* 13.1, 13.2; ►*NYS P03-002*, Part 6; ►*GLBA* 314.4(a)(b)(3); ►*GLBA IG* III(C)(1)(g); ►*HIPAA* 164.308(a)(6)(i); ►*PCI* (12).

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 *Standards for Internal Control in New York State Government*

Industry Standards:

Payment Card Industry Data Security Standard (PCI-DSS)
ISO 27001 and ISO 27002

Related Procedures and "Other Requirements"

Internal Control Program Guidelines, Document #7501

History

February 1, 2008, Procedure established

Appendices

A. References
B. Program Documents
C. University Declaration of Sensitive Information
D. History of Related Legal Requirements for University Information Security Management
E. Sample Entries for a Catalog of Practices & Protections
F. Confidentiality Practices and Protections in New York State Policy
G. Information Security Practices Recommended by New York State (*Word*)
H. Information Security Practices Recommended by New York State (*Excel*)

Definitions

The following terms are defined solely for the context of this Procedure. In the text, many are capitalized and put in quotation marks.

- **Analysis of Practices and Protections** – a professionally and legally sound analysis of required, existing, and missing practices and protections (see definition) that mitigate or otherwise address the risks identified in the Risk Analysis. Also the Program Document that records this analysis.
- **Asset Inventory** – a set of records presenting to the Program the risk-oriented facts, such as location, owner, users, custodians, business value, sensitivity, and backup information, regarding the most critical forms of Sensitive Information and Sensitive Systems.
- **Campus** – a college, school, or university of the State University of New York.
- **Catalog of Practices and Protections** – a Program Document providing concise descriptions of identifiable practices and protections (see definition) with sufficient detail to enable managers, the general workforce, faculty, and students to identify and work effectively with the instances of each item in their domains.
- **Colleagues** – key managers of the major business functions of a Campus.
- **HIPAA-covered SUNY Campus** – a Campus that the University has formally determined is covered under HIPAA. Such determination is based on the Campus's having identified at least one business function that meets the University's interpretation of HIPAA-covered, which in most cases is due to creating and/or having authorized access to *protected health information* (PHI) as defined by HIPAA. Most PHI is personal health records created or used in electronically billed health transactions conducted by Campus personnel.
- **Incident Response Team** – a formal group defined and maintained by the Program that readies the Campus to respond quickly and appropriately to security incidents, which are sudden, unplanned, adverse, locally impacting changes that threaten the security of Sensitive Information and Sensitive Systems and therefore require urgent and timely mitigating responses.
- **Information Security Program** – a formal management function, with written goals and charges, that seeks to address the full range of information security issues that affect the Campus and seeks to align its practices with applicable laws, regulations, policies, and standards of practice.
- **ISO** – Information Security Officer/Office/Oversight. An assigned person (Officer) or group (Office) or coordinated function (Oversight) that understands the Campus's information security risk, the Program, and the meaning and intent of the University standards for information security and who presents professionally and legally sound and timely advice to executive management regarding appropriate action, ensuring the Program is exposed to outside, professional perspective, especially that of the University's central information security oversight function.
- **Practices and Protections** – individual and group behavioral patterns (practices), such as using hard-to-guess passwords, and system/infrastructure configuration and tools (protections), such as anti-virus software, maintained by the Campus to remove or reduce the impact of threats to the security of its Sensitive Information and Sensitive Systems.
- **Program** – the Campus's information security program.
- **Program Document** – one of several major documents or sets of documents generated or maintained by one part of the Program and needed by another part of the Program.

- **Professionally and legally sound** – the characteristic of a Program whereby professional and legal information security analysts would find its structure, analysis, decisions, and responses reasonable and appropriate.
- **Risk Analysis** – a formal process of the Program wherein the Campus considers and records foreseeable threats and hazards, especially those that are well known and have high likelihood and impact, that could result in substantial harm or inconvenience to the University or to persons who are the subject of the personal information in its Asset Inventory. Also the Program Document that records this analysis.
- **Senior Executive** – one or more Campus executives with power to commit Campus funds and personnel that approve and oversee the Program.
- **Sensitive Information** – a *policy*-level security classification used by the University and Campuses to name in aggregate the formally declared set of *standards*-level categories of information, such as Social Security Number, being addressed, i.e., protected, by the Program.
- **Sensitive System** – a physical or digital container of Sensitive Information, such as a computer, network, database, application, building, room, cabinet, or other configurable component of the Campus infrastructure directly involved in the sheltering (i.e., housing and locking), storing, processing, or transmitting of Sensitive Information.
- **University** – the State University of New York.
- **Workforce Inventory** – a set of records regarding the workers having authorized access to the Sensitive Information and Sensitive Systems (i.e., the items presented in the Asset Inventory), presenting to the Program the risk-oriented facts, such as work location, work group and supervisor, security roles and object authorizations.