Program Documents
Appendix B, *Information Security Guidelines, Part 1, Campus Programs & Preserving Confidentiality,* Document #6608.
Responsible Office: Administrative Services and Technology
February 1, 2008

This appendix provides further guidance regarding the content and purpose of each of the 12 "Program Documents" introduced in Standard A4 in the Procedure. Program Documents are the set of strategic and operational documentation that are the critical records and reports arising from the actions required by the Standards in the Procedure. While this term applies to *any* of the documents produced by the work of the Program, the term more closely refers to the 12 documents named in Standard A4.

Taken as a whole, the set of Program Documents answers for the campus the following critical question: "When the law and professional standards say that information security programs must be '*written*' what does that mean; *what* does one write?" Laws and the information security profession leave us largely on our own to answer that question in our own ways. The University has done so as well, in the past. But now, with its first information security guidance procedure, it provides some significant detail to the question, *What* does one write? It does so while still leaving campuses appropriate degrees of freedom to "determine the precise content, formatting, and names for their Program Documents" (A4).

The Procedure seeks to guide the campus in becoming *dynamic* in its handling of risk, to be nimble and responsive to the changing nature of threats, assets, and methods of protection. No static set of "Do This" documents would suffice in creating such dynamism. It requires an active system of reading and writing, thinking and acting, input and output. In short, it requires a "learning organization." The Program Documents are essential components of that learning, as suggested by their formal definition:[1] "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" (italics added). This feature of "generating" in one place, and "needing" in another is a key feature of a learning organization.

The Procedure gives campuses wide latitude in all aspects of Program details, including its written output. Therefore, campuses may determine for themselves (or collaborate to design) the precise structure, content, and format of these 12 documents. The documents should, however, express the clear intentions and design of the Program as expressed in the Procedure. This appendix takes a first step in that direction. It gives campuses further guidance, not only in writing specific documents, but more importantly in using documents to stimulate a learning organization.

Each of the 12 Program Documents requires detailed planning regarding content and presentation. One must consider, for example, whether a document should best be put into tables that can be sorted, as in a spreadsheet, or in a hierarchically presented narrative, as in an outlined word document. Because many of the Program Documents are hand-off points between Program functions, designers must enable these files to meet both the needs of the people who create the

[1] see the Procedure's Definition section for "Program Document."

files as well as the ones who use them. These are often adjacent Standards in the Procedure. For example the *Asset Inventory* created in C1 is immediately used by the creators of the *Workforce Inventory* in C2. Both of these are then used in risk analysis in D1. To assist campus designers to see the whole picture right away, key interdependencies are indicated in the Action of, Input from, and Output to entries for each document.

> Action of lists the Standard that calls for creating this document.
>
> Input from is an abbreviated list of sources the document makers will use or need. These sources may be actions of another Standard, a Program Document, existing campus documents, people, organizations.
>
> Output to is a short list of other actions and documents that will use or need this document. A notation with ">" between Standards, e.g. "C1>C2>D1>D2>E1" indicates the natural "food chain" where the output of the document feeds another function and through that, closely influences all that follows it.

The action, input, and output fields for each Document are extracted in the following table:

1. *Program Authorization*:

> Action of: A1; A2; A3; A4.
> Input from: campus policy; job descriptions; Procedure.
> Output to: All parts of the Program; B1; B2; E1; OISO.

2. *Program Documentation Plan*

> Action of: A4.
> Input from: Appendix B (this document); the Procedure.
> Output to: OISO; All parts of the Program.

3. *Sensitive Information Categories*

> Action of: B1.
> Input from: University declaration (Appendix C); campus policy.
> Output to: B2 policies; C1>C2>D1>D2>E1>E2>E3.

4. *Policy and Standards*

> Action of: B2.
>
> Input from: Procedure; existing University and campus policy; law.
> Output to: All parts of the Program.

5. *Asset Inventory*

> Action of: C1.
> Input from: B1 *Sensitive Information Categories;* other inventories.
> Output to: C2 workforce inventory; D1>D2>E1>E2>E3.

6. *Workforce Inventory*

Action of: C2.
Input from: C1 *Asset Inventory.*
Output to: D1 risk analysis; D2>E1>E2>E3.

7. *Risk Analysis*

Action of: D1.
Input from: C1; C2; D2 analysis of practices and protections.
Output to: E1; E2>E3; D2 analysis of practice and protections.

8. *Catalog of Practices and Protections*

Action of: D2.
Input from: Procedure D2 categories (*a* through *m*); standards of practice; campus practices; University templates.
Output to: D2 analysis of practices and protections.

9. *Analysis of Practices and Protections*

Action of: D2.
Input from: D2 *Catalog of Practices and Protections.*
Output to: D1 *Risk Analysis;* E1 decisions and projects.

10. *Summary of Project Plans and Outcomes*

Action of: E1; E2; E3.
Input from: D1 *Risk Analysis;* E1 decisions and projects.
Output to: OISO; D1 risk analysis; D2 analysis of practices and protections.

11. *Training & Awareness Plan and Record*

Action of: E2.
Input from: E1 project charges.
Output to: D1 *Risk Analysis;* E1 decisions and projects.

12. *Incident Response Plan*

Action of: E3.
Input from: E1 project charges.
Output to: E3 Incident Response Team; D1 *Risk Analysis;* E1 decisions and projects.

Program Organization (Standards A1-A4)

1. *Program Authorization*

Description: The document provides formal statements that authorize and define the campus Program. It establishes responsible parties by job function and name or cites a related document that gives that information. It is signed by a senior executive. The text could be placed inside a campus policy (B2) document, and in any case is treated like policy in the way it is written, stored, and communicated. Unless it predates the Procedure, it should cite the Procedure as an authorized guide for the Program.

Action of: A1; A2; A3; A4.

Input from: campus policy; job descriptions; Procedure.

Output to: All parts of the Program; B1; B2; E1; OISO[2].

Example: *ISec_Program_Controlling_Document-Sample.doc* is a version of this type of document provided as a template prior to the Procedure, October 2006.

2. *Program Documentation Plan*

Description: The document provides a plan and table of contents for the 12 Program Documents, including the documents' owners, storage locations, status, and planned/actual completion dates. The document helps the Program planners and managers organize the important inputs and outputs of the Program's various functions.

Action of: A4.

Input from: Appendix B (this document); the Procedure.

Output to: OISO; All parts of the Program.

Policy & Standards (Standards B1, B2)

3. *Sensitive Information Categories*

Description: The document lists the categories of information the campus formally declares are "Sensitive Information" (SI)[3]. The document carries the authority of campus policy, which it creates with statements inside the document as well as policy statements made elsewhere regarding the role and authority of the listing. The document lists standards-level business categories (see Detail, below) and includes all categories declared by the University (see Appendix C). The categories assist students and workers to identify specific types of information that require special care and to detect incidents and improper conduct.

Action of: B1.

[2] OISO = System Administration's office for information security oversight which includes action by the University-wide Information Security Officer, University auditors, and the Chief Compliance Officer.
[3] See the Procedure's Definition section for "Sensitive Information."

Input from: University declaration (Appendix C); campus policy.

Output to: B2 policies; C1>C2>D1>D2>E1>E2>E3[4].

Detail: The University *Declaration of Sensitive Information* (Appendix C) lists categories in what might be termed "standards-level business categories" which are categories defined by law, regulation, or policy. The categories are generally applicable to all entities covered by a specific standard, such as HIPAA, FERPA, and GLBA. The information categories apply to specific business functions, such as health transactions, registration, financial aid. For example, the FERPA-related entry is "*personally identifiable information on students in education records as defined in the Family Educational Rights and Privacy Act.*" In addition to that type of entry, the document may include categories that cut across several standards, such as "*Social Security Number paired with personally identifying information*."

To locate instances of SI, Program operations, such as C1 asset inventory, need categories based on operational details specific to the campus. These *procedure*-level categories are described in the detail under *Asset Inventory*.

4. *Campus Information Security Policy*

Description: These are authorized, executive statements regarding the campus's position on the protection of Sensitive Information and Sensitive Systems. These texts may take any form that suits the campus. The statements should be professionally and legally sound. Policies released or updated after the Procedure, should reflect the required actions described by the Procedure.

Federal (PRISMA) guidelines state that information security policies should be formal, up-to-date, stated as "shall" or "will," be readily available to employees, and be approved by key affected parties. They should cover all major facilities and operations, agency-wide, or for a specific asset, should delineate the information security management structure, clearly assign information security responsibilities, lay the foundation necessary to reliably measure progress and compliance, establish a continuing cycle of assessing risk and monitoring program effectiveness, and identify specific penalties and disciplinary actions to be used if the policy is not followed.

Action of: B2.

Input from: Procedure; existing University and campus policy; law.

Output to: All parts of the Program.

Example: NYS Information Security Policy; various SUNY campus policies;; Educause; NIST.

Detail: A comprehensive information security policy may consist of a single document, such as NYS's policy, or be a set of policies, each dealing with specific

[4] The notation introduced here with the ">" between Standards, e.g. "C1>C2>D1>D2>E1" indicates the natural "food chain" where the output of a document feeds another function and through that, closely influences all that follows it. Here, the declaration of SI influences B2 (policy) and C1 (asset inventory) but from there on influences closely all the other analysis and decisions.

issues or addressing specific audiences. A new policy could contain key statements from the *Program Authorization* and cite the *Sensitive Information Categories* document.

Inventory (Standards C1, C2)

5. *Asset Inventory*

Description: This document presents a risk-oriented, itemized enumeration of the sensitive assets that meet the categories declared sensitive by the campus in its *Sensitive Information Categories*. It includes the instances of information that must be protected and the systems that house it[5]. The documents are oriented, designed, and formatted to the needs of risk analysis. The Procedure suggests the inventory should include at least asset type, location, owner, users, custodians, business value, sensitivity, and backup information. If several separate domains of the campus are doing separate risk analysis and mitigation (C1 through E3), then these domains may define individual formats for their *Asset Inventories* and *Workforce Inventories*.

Action of: C1.

Input from: B1 *Sensitive Information Categories;* other inventories.

Output to: C2 workforce inventory; D1>D2>E1>E2>E3.

Detail: To create the asset inventories, analysts need what might be called "procedure-level business categories." These categories name details specific to the campus's business procedures. Analysts start, as they must, with the policy categories (B1) such as "Social Security paired with personally identifying information." They then consider how that appears in the business of the campus. For each distinct type, they name a procedure-level business category, such as "*Student* Social Security Number stored or accessed with *Student* Name in {*our Student Information System.*}" Then they make the other, parallel categories that address SSN of other persons, such as employees, alumni, parents, and applicants. Each of these categories is worth identifying because the information may be located and processed in different systems and have different owners, locations, systems, and workers with access rights. They use these procedure-level business categories to interview business functions regarding ownership, etc., and IT functions regarding systems.

6. *Workforce Inventory*

Description: This document presents a risk-oriented, itemized enumeration of the workers with authorized access to the objects in the *Asset Inventory*. The documents are oriented, designed, and formatted to the needs of risk analysis. The Procedure suggests the inventory should include at least work location, work group and supervisor, security roles and object authorizations. As noted above, separate

[5] See the Procedure's Definition section for "Sensitive System."

domains of the campus may do separate risk analysis and mitigation (C1 through E3) and define separate inventories.

Action of: C2.

Input from: C1 *Asset Inventory.*

Output to: D1 risk analysis; D2>E1>E2>E3.

Analysis (Standards D1, D2)

7. *Risk Analysis*

Description: These documents present the thinking and conclusions of a specific risk analysis governed by the Program at a given point in time that assessed the risk in a specific domain of the campus. *Risk Analysis* documents provide subjective-but-educated answers to, "What are the significant and likely things that could go wrong with our assets, given what we currently know about the protections we have in place?" The Procedure, being oriented to Confidentiality, requires at least an analysis of "what could go wrong" that considers how workers and systems could allow SI to be stolen or leaked.

The *Risk Analysis* documents' content and structure reflect the specific risk analysis method used in the process, and these processes are defined by the campus or department undertaking the analysis. The outputs of the analysis should be oriented, designed, and formatted to the needs of the executives and analysts who decide how the campus or a domain will respond to risk, as required in E1. The two other analysis documents in D2 (catalog and analysis of practices and protections) serve the D1 function. But previous analysis may be used by D2.

Action of: D1.

Input from: C1; C2; D2 analysis of practices and protections.

Output to: E1; E2>E3; D2 analysis of practice and protections.

Detail: Risk analyses must have focus in time and place to be meaningful. They therefore can occur simultaneously in different domains (e.g., schools, departments, sub-campuses) and can proceed independently of each other and use differing methods. In every case, however, the process and the output must be crafted to serve the needs of decision makers who will be making E1 responses for that domain.

8. *Catalog of Practices & Protections*

Description: The document provides itemized, concise descriptions of practices and protections that are well known in the information security profession and that apply to similar organizations as well as ones that apply or could apply to the campus. The Catalog provides answers to, "What types of things do similar organizations do to protect their information and systems, and how are these

applied here?" Entries are made by campus managers in the various areas of practice and briefly summarize current campus implementations.

To "ensure the Program is exposed to outside, professional perspective" (Standard A1), the catalog builders proactively study and draw from entries of generally accepted ("best practices") made in a University-maintained catalog which is created through a transparent, collaborative process by information security experts within the University who track developments in the field (e.g., from the law, international and federal standards, Educause, SANS).

The Procedure's text in D2 provides 13 categories (*a* through *m*) the analysts making the Catalog must consider. These are *categories* of practice and protection, not *instances* of them. The Catalog is oriented, designed, and formatted to the task of building the Catalog, but also to the needs of the analysts who use the Catalog to do *Analysis of Practices and Protections*.

Action of: D2

Input from: Procedure D2 categories (*a* through *m*); standards of practice; campus practices; University templates.

Output to: D2 analysis of practices and protections.

Detail: For example, statements entries regarding learning and training of the general workforce are made by managers assigned to oversee or provide that kind of service to members of the community. Statements regarding the many IT security items in the catalog are made by campus IT managers in the specific practices, such as Linux system administration, web design, networks.

Federal (NIST) standards contain many practices and protections that may be freely used and copied. The NYS Information Security policy may be used and copied as may the 300 practices SUNY has derived from that (see Example). The Information Security Forum's *Standard of Good Practice* is free for use within a campus if the text is not copied for public access. Specific practices in IT have detailed practice checklists in NIST, the Center for Internet Security, and many other sources.

Example: Appendix E. *Sample Entries for a Catalog of Practices & Protections*

9. *Analysis of Practices & Protections*

Description: These documents present the thinking and conclusions of a specific analysis regarding the practices and protections in the campus's *Catalog of Practices and Protections*. It states which of these items are in place in a given domain and of the ones that are missing, states which are required or otherwise important, reasonable, and appropriate for the campus. The analysis does not assert what is thought to be actually feasible at this time, which is done in meetings of managers and recorded in minutes.

Action of: D2.

Input from: D2 *Catalog of Practices and Protections.*

Output to: D1 *Risk Analysis;* E1 decisions and projects.

Detail: Compliance tools can be used as the catalog and an assessment. The federal PRISMA is an example.

Practices & Protections (Standards E1, E2, E3)

10. *Summary of Project Plans and Outcomes*

Description: This document or set of like documents provides management-level summaries regarding what has been done and is planned to be done to address the findings of the previous *Risk Analysis*. The reports express purposes, costs, owners, and timelines of the projects. It also summarizes outcomes of projects and gives updates to reflect the ongoing degree of usefulness of the practices and protections that were the subject of a previous project. The documents are oriented, designed, and formatted to the needs of the executives and analysts who initiated the projects, and also are used in subsequent rounds of D1 and D2 analysis.

Action of: E1; E2; E3.

Input from: D1 *Risk Analysis;* E1 decisions and projects.

Output to: OISO; D1 risk analysis; D2 analysis of practices and protections.

11. *Training & Awareness Plan and Record*

Description: The document outlines the plans for actions that raise awareness about information, system, and cyber security and promulgate skills for successfully implementing practices and protections. It also records major actions. These are management documents made in any format most useful for those who read and use them.

Action of: E2.

Input from: E1 project charges.

Output to: D1 *Risk Analysis;* E1 decisions and projects.

12. *Incident Response Plan*

Description: The document outlines the plans for actions that that prepare campus workers and students to respond to incidents in information, system, and cyber security. It also records major actions. These documents are oriented, designed, and formatted to the needs of management and the members of the Incident Response Team.

Action of: E3.

Input from: E1 project charges.

Output to: E3 Incident Response Team; D1 *Risk Analysis;* E1 decisions and projects.