Confidential Data Handling Blueprint

Version 2.0: September 2009

Purpose

To provide a toolkit that constructs resources pertaining to confidential data handling. Many of the EDUCAUSE/Internet2 Higher Education Information Security Council (formerly the Security Task Force) working groups are working on components of the toolkit, but this consolidation and organization of resources anchors the overarching themes related to information protection.

Introduction

The following steps and ensuing sub-items are intended to provide a general roadmap. Institutions will be at varying stages of progress. Some will start with the need to establish actions in the areas of policies, processes, or technology. Some will be ready to implement, and some will be able to revise and fine-tune their processes. You will also need to prioritize your actions to mitigate risks because of the comprehensive nature of the recommendations. We've attempted to organize these in a sequence that allows you to logically follow through each step. Although each item is recommended as an effective practice, we recognize that state/local legal requirements, institutional policy, or campus culture might cause each institution to approach this differently.

Definition - "Confidential Data"

Confidential data includes both sensitive personal information and sensitive institutional information. Unauthorized access to personal confidential data may result in a significant invasion of privacy, or may expose individuals to significant financial risk. Unauthorized access to or modification of institutional confidential data may result in direct, materially negative impacts on the finances, operations, or reputation of the institution. Examples of personal confidential data include information protected under privacy laws, information concerning the pay and benefits of employees, personal identification information, medical/health information held by the institution pertaining to those affiliated with it, and data collected in the course of research on human subjects. Institutional confidential data, for example, includes institutional financial and planning information, legally privileged information, invention disclosures, and other information concerning pending patent applications.

Definition - "Policy", "Standard", "Procedure"

This document makes use of all 3 terms, and they are *not* synonomous. For the purposes of this document, a policy is a relatively abstract statement of a goal. A standard is a group of specific technical settings, protocols, vendors, or benchmarks. A procedure is a set of specific operating instructions. Standards and procedures are frequently developed to support policies, but can also stand alone in some situations.

For example, an institution might have a policy that states that all confidential data must be encrypted. It might also have a standard that states that the encryption must use the AES cipher with a key length of 256 bits for file encryption and use the TLS/SSL protocol for network entcryption using the AES or Blowfish ciphers, or simply require use of software "XYZ" (which is available correctly configured) to encrypt data. Finally, a procedure would give specific instructions for ensuring that the encryption policy and standards are being implemented correctly..."To encrypt a file, run this program from the server, choose the filename, choose a password, and click 'OK'," or "To ensure that your network traffic is encrypted, look at the bottom of the browser for an icon of a padlock. If it is not there, call the Help Desk at 555-1212 to report a problem."

Steps

Step 1: Create a security risk-aware culture that includes an information security risk management program

Statistics consistently show that the lack of security awareness and management attention to security are frequent causes of data exposure incidents. Subsequent steps in the Blueprint should significantly lower the risk of such incidents. The risk reduction, however, will be short-lived unless everyone in the institution assumes responsibility for protection of institutional data and executives and managers fully appreciate and act on the fact that strong security programs have a direct positive impact on such critical institutional issues as:

a. Meeting organizational goals
b. Maintaining efficient, uninterrupted operational processes
c. Fostering a positive public image
d. Complying with legal statutes, regulations, contractual obligations

Sub-Step	Resource	Resource Type

1.1 Institution-wide security risk management program. An institution-wide security risk management program should include information, templates, and tools to guide the completion of an impact analysis for institutional data assets, a risk assessment for those assets, and continuity planning for events that could damage the assets or otherwise make them unavailable. Completing such a risk management process provides insight into existing risks within a given IT environment and strategies for reducing or eliminating those risks. Implementing a policy that requires organizational units to cycle through the program on a regular schedule helps insure managers stay abreast of changing risks and respond accordingly.	Tool: Risk Management Framework	Higher Education
	Tool: Information Security Program Self-Assessment Tool	Higher Education
	Policy: Harvard University's Enterprise Security Policy	Higher Education
	Info: National Infrastructure Protection Plan (NIPP)	Government
	Policy: NIST Risk Management Guide for Information Technology Systems (SP 800-30)	Government
	Policy: NIST Managing Risk from Information Systems: An Organizational Perspective (DRAFT SP 800-39)	Government
1.2 Roles and responsibilities defined for overall information security program at the central and distributed level. In a culture of security risk awareness, all individuals within the institution understand their roles and responsibilities for protecting data to which they have access. These roles and responsibilities should be clearly stated and communicated, and individuals should be held accountable for fulfilling them. Certain individuals, for example in the Registrar's office or in the central IT organization, will likely have greater security responsibilities than others, but everyone in the institution must personally assume some responsibility for the security of institutional data in electronic and/or paper form.	Policy: Indiana University Trustees Resolution	Higher Education
	Policy: Indiana University School of Medicine Roles	Higher Education
	Policy: Yale University Information Access and Security Policy	Higher Education
1.3 Executive leadership support in the form of policies and governance actions. In today's environment funding for security is commonly considered a "sunk cost" and security resources are focused primarily on reactive, band-aid tactics. In an institution that is security risk-aware, however, security would be viewed as an investment in the mission of the institution and security resources would be focused on proactive, risk management based strategies. Making a transition to a culture of security risk awareness can be enabled through the adoption of a governance model for security that integrates the security program into overall goals, objectives, and operational processes of the institution.	Info: Information Technology Security: Governance, Strategy, and Practice in Higher Education	Higher Education
	Info: Governing for Enterprise Security article series - Carnegie Mellon Software Engineering Institute	Research

#Top of page

Step 2: Define institutional data types.

A thorough understanding of the different information resources maintained and used by an institution is a key aspect of determining the requirements for protection of confidential data. Typically data types are grouped such that controls may then be applied in a manner that is commensurate to reduce financial, legal, and reputational risks to the institution.

Sub-Step	Resource	Resource Type
2.1 **Understand the legal and regulatory landscape.** An important consideration when safeguarding the privacy and security of data held by an institution (and outside parties on its behalf) is complying with applicable federal, state, and international laws and regulations related to the privacy and security of the data held by the institution, as well as any contractual protection obligations that may exist. Specific security controls are often legally prescribed for various data types, and these must be taken into consideration when developing a protection plan.	Info: Policing the Internet: Higher Education Law and Policy	Higher Education
	Info: Liability for Negligent Security	Higher Education
	Info: Gramm-Leach-Bliley	Higher Education
	Info: HIPAA	Higher Education
	Info: FERPA	Higher Education
	Info: FACTA Red Flag Rule	Government
	Info: State Security Breach Notification Laws	Government
	Info: Data Breach Notification Laws by State	Industry
	Info: Payment Card Industry (PCI) Security Standards Council	Industry
2.2 **Develop a classification system.** A data classification schema must be developed with input from legal counsel and data stewards as defined in section 3.1. Consistency and reliability of controls and clarity of responsibility are achieved by developing a schema which can be applied to any data type, but which allows for individual exception.	Policy: Data Classification Policies	Higher Education
	Tool: Risk Management Framework	Higher Education
	Info: SANS Information Sensitivity Policy	Industry
2.3 **Apply the schema.** Using the schema, a classification is assigned to institutional data to the extent possible or necessary. Assignment involves review and subsequent documentation of data types and their information sensitivity classification.	Info: Iowa State University Data Classification and Retention System	Higher Education
	Tool: Classifying Institutional Data	Higher Education

	Info: FIPS 199	Government
	Info: SANS Information Sensitivity Policy	Industry

#Top of page

Step 3: Clarify responsibilities and accountability for safeguarding confidential data

Along with understanding and grouping information resources, assigning responsibility for those resources is a critical component to ensure that they are properly handled.

Consider a file of employee salary information as an example. This file could be the responsibility of the central Human Resources Department, which maintains master files. It could also be the responsibility of Information Technology, which maintains the human resources information system, or of departmental staff who maintain local human resources files. Responsibility might also be split between these entities.

Sub-Step	Resource	Resource Type
3.1 **Data stewardship roles and responsibilities**. It is not sufficient to have a classification system as delineated in *Step 2*. Individuals both at the user level and in management must understand their role in classifying and protecting the data. Consider adding such responsibilities directly to the formal job description for key roles.	Policy: Data Classification Policy of the University of North Carolina at Greensboro	Higher Education
	Policy: Boston College Data Security Policy	Higher Education
3.2 **Legally binding third party agreements that assign responsibility for secure data handling.** If you give confidential data to an outside party, for example, to maintain student loans, or develop a web site, or handle health insurance, you need to ensure in a contract that the other party understands that it is liable for properly safeguarding the information. The 2008 Verizon Business Data Breach Report, based on analysis of over 500 actual breaches, showed that 39% of the breaches stemmed from a business partner. While not legally binding, obtaining a SAS-70 statement, SAS-112 procedures, or a form from the BITS Shared Assessments program is helpful in gauging the strength of an outside party's data handling measures.	Info: Third Party Contractual Language	Higher Education
	Info: The Third Party Network Connection Agreement	Industry
	Info: Application Service Provider Standards	Industry
3.3 **Develop policies and assign accountability for data retention, data disposal, and electronic discovery**. Data has its own "life cycle" from its collection to its eventual disposal. Your policies should describe data handling at significant points in this cycle.	Info + Policy: Ohio State University Records Management	Higher Education
	Policy: Cornell Retention of University Records	Higher Education
	Policy: Harvard secure disposal policy	Higher Education
	Info: EDUCAUSE Review article - Electronically Stored Information and the Federal Rules of Civil Procedure	Higher Education

	Tool: Guidelines for Information Media Sanitization	Higher Education

#Top of page

Step 4: Reduce access to confidential data not absolutely essential to institutional processes

One of the most effective means of not accidentally exposing confidential data is simply reducing access to the data. This includes not collecting such data if not absolutely necessary, not showing it on printed reports or computer screens, and eliminating cases where it has been historically stored in locations, both electronic and paper, where it is no longer required.

Sub-Step	Resource	Resource Type
4.1 **Establish, apply and maintain policies and procedures for data collection processes (including forms) to request only the minimum necessary confidential information.** Not requesting nor collecting restricted/regulated data is the best method of ensuring that it is not leaked -- an organization doesn't have to worry about protecting (in storage or transit) what it does not have. This should apply to online and paper forms.	Info: EDUCAUSE FERPA resources	Higher Education
	Policy: EDUCAUSE /Cornell ICPL Policies	Higher Education
	Info: 2008 FERPA Final Rule (PDF, HTML)	Government
	Policy: SANS Information Sensitivity Policy (PDF, MS Word)	Industry
4.2 **Establish, apply and maintain policies and procedures for application outputs (e.g., queries, hard copy reports, etc.) to provide only the minimum necessary confidential information.** In many or most cases an analysis of the information which is absolutely essential on a report or screen will reveal that full or even partial confidential information which is superfluous (e.g., an employee SSN on a pay stub is not needed and is a liability; a partial credit card number or the last few digits of a bank account are usually all that is needed on a payment screen when displaying a transaction).	Policy: Data Classification Policies	Higher Education
	Tool/Info: Data Classification Toolkit	Higher Education
	Info: NIST 800-60 (Rev. 1 2008): Guide for Mapping Types of Information and Information Systems to Security Categories (Guide, Appendices)	Government
	Info: New Zealand Government "Information Classification".	Government
	Info: Sun Blueprint Series "Data Security Policy - Structure and Guidelines"	Industry
	Info: Shon Harris on "Drafting Data Classification Policies and Guidelines"	Industry
4.3 **Inventory and review the presence of existing confidential data on servers, desktops, and mobile devices.** Use data scanning tools and store/update the results in a database. IT GRC (Governance, Risk and Compliance) software now exists which can maintain an asset inventory database of confidential data sources and systems.	Info: Baylor University IT Asset Management Presentation	Higher Education
	Tool: Cornell University Spider	Higher Education

	Info: Northwestern University's Guideline for Using Sensitive Data Search Tools	Higher Education
	Tool: University of Illinois at Urbana-Champaign Firefly SSN Finder for Windows	Higher Education
	Tool: University of Texas at Austin Sensitive Number Finder (SENF)	Higher Education
	Tool: Virginia Tech Find_SSNs Tool	Higher Education
4.4 **Establish, apply and maintain policies and procedures to eliminate unnecessary confidential data on servers, desktops, and mobile devices.** Initiate a confidential data elimination project if there is not a continuous process currently in place.	Policy: SANS Information Sensitivity Policy (PDF, MS Word)	Industry
4.5 **Eliminate dependence on SSNs as primary identifiers and as a form of authentication***	Info: Elimination of Social Security Numbers As Primary Identifiers	Higher Education
*Note: SSNs may need to be used for certain things (e.g., student employees, student financial aid, etc.) and we recommend that schools limit the use of SSNs to only necessary processes	Tool: UCONN SSN Elimination Project Action Plan	Higher Education

#Top of page

Step 5: Establish and implement stricter controls for safeguarding confidential data

Controls provide enforcement of higher level policy via either detailed procedure(s), technological mechanism(s), or both. A high level policy or assignment of responsibility does not actually protect confidential data; detailed controls provide the protection.

Sub-Step	Resource	Resource Type
5.1 **Inventory and review/remediate security of computing resources**. For network resources, segregate guest access and block unrestricted access to wired and wireless networks unless a known user logs in. For computational resources, consider testing computers upon network access to verify that they are fully patched.	Tool: NetReg	Other
5.2 **Establish and maintain standards for the security configuration of computing resources.** This includes applications, servers, desktops, and mobile systems. It also includes network resources such as firewall, intrusion detection/prevention, and router configurations. Note that "standards" are *not* "policies" -- standards are specific, prescriptive lists of appropriate settings that change as the base of computing resources change, whereas policies tend to be both more general and more static over time.	Policy: Harvard policy on Internet access to confidential information	Higher Education
	Info: NIST user guide for securing external devices	Government
	Info: NIST guide to general server security	Government
	Info: NIST guide to secure web servers	Government
	Info: NSA configuration guidelines	Government
	Info: CIS Benchmarks	Industry
	Info: NIST guidelines on firewalls and firewall policy	Government
	Info: Network devices	Government

5.3 **Establish and maintain encryption standards and strategies for data in transit and at rest.** If data is confidential, it is usually beneficial to encrypt it to protect it from unauthorized access, either as it transits networks, as it is stored in files or databases, or both. In some cases, such as credit card data, encryption is contractually required.	Policy: Yale University IT Acceptable Use Policy (see Section F for Data Encryption Policy)	Higher Education
	Tool: Yale University Endorsed Encryption Implementation Procedure	Higher Education
	Policy: Harvard Enterprise Security Policy - section 2.3	Higher Education
	Policy: Cryptographic Standards and Application	Industry
	Policy: SANS Acceptable Encryption Policy	Industry
5.4 **Establish and maintain standards regarding (a) confidential data on mobile devices and home computers, and (b) data storage and archiving.** These areas are frequently overlooked, and are also frequently the source of a data loss.	Policy: Harvard Central Admin. remote access policy	Higher Education
	Policy: SANS remote access policy	Industry
	Policy: SANS mobile device encryption	Industry
5.5 **Establish and maintain policies concerning identity management and resource provisioning processes.** Improper issuance of user credentials and improper controls over user access to resources can lead to unauthorized access by users who have access privileges but should not, or who have a login but also have access to systems or data they should not have such access to. Improper revocation of credentials and keys is as critical an issue as improper issuance, and must also be addressed fully.	Info: EDUCAUSE Spotlight on Identity Management	Higher Education
	Info: InCommon	Higher Education
	Info: EDUCAUSE Identity and Access Management resources	Higher Education
5.6 **Establish and maintain technical procedures for data retention and secure disposal of equipment and data.** Step 3.3 covers policies for data retention and disposal. It is also necessary to have detailed technical procedures. Computers, disk drives, tapes, and other data are all too often donated to charity, sent to a dump, or sold as surplus with confidential information intact on them. Technical procedures might include how to archive old documents and what specific steps should be taken to sanitize media prior to disposal.	Policy: Harvard secure disposal policy	Higher Education
	Info: NIST guidelines for media sanitization - in revision	Government
	Policy: NIST records management policy	Government
	Info: an electronic record retention policy: no longer a luxury	Industry

5.7 **Consider performing background checks on individuals handling confidential data.** Persons with criminal records or credit histories indicating an inability to handle money responsibly may not be ideal candidates to handle confidential data. Yet many institutions do not perform any checks on employees or potential employees handling confidential data. This is a sensitive topic at many institutions, thus the "consider" in the statement.	Info: EDUCAUSE: background checks	Higher Education
	Info: PCI background check requirement	Industry

#Top of page

Step 6: Provide awareness and training

Assure that training requirements for each law, regulation, or control are being met. Build a list of training requirements that shows who must be trained based on what topics.

Sub-Step	Resource	Resource Type
6.1 **Make confidential data handlers aware of privacy and security requirements**. Changes to regulations for data privacy and security must be communicated to the affected areas of the higher education community.	Info: NIST SP800-50: Building an Information Technology Security Awareness and Training Program, October 2003	Industry
6.2 **Require acknowledgment by data users of their responsibility for safeguarding such data.** Each person with access to confidential information should be presented with an acknowledgment to ensure understanding their role, whether its as a consumer/user of information, a creator of information, or a steward/manager of information.	Policy: Confidentiality Agreement or Statement Policy: Template Non-Disclosure and Confidentiality Agreements (Texas State University, San Marcos)	Higher Education
6.3 **Enhance general privacy and security awareness programs to specifically address safeguarding confidential data.** A key component of any awareness program is instruction regarding the data sensitivity classifications for information as defined by your institution. In addition, the controls and safeguards for each confidential data classification should be described.	Info: Campus-wide Security Education and Awareness (Chapter 7 in the online book "Computer and Network Security in Higher Education")	Higher Education
	Info: NIST SP800-50: Building an Information Technology Security Awareness and Training Program, October 2003	Industry
6.4 **Clearly communicate how to safeguard data** so that collaboration mechanisms, and their respective strengths and limitations in terms of access control, are clearly understood.		

#Top of page

Step 7: Regularly verify compliance with your policies, standards, and procedures

Assure that requirements for each data element or system are being managed. Build a list of compliance requirements that indicates which data elements (or systems) the requirements apply to and which data steward (or person) is responsible for each requirement.

Sub-Step	Resource	Resource Type
7.1 **Conduct regular meeting**s with stakeholders such as data stewards, legal counsel, compliance officers, public safety, public relations, and IT groups to review institutional risk and compliance and to revise existing policies and procedures as needed		
7.2 **Utilize audit function within the institution** to verify compliance. This can be either an internal audit department or external auditors.	Info: Auditing and Assessment	Industry
7.3 **Routinely scan and test computing resources and services.** Scan servers, desktops, mobile devices, and networks containing confidential data to verify compliance with institutional policy and standards. Test these devices for weaknesses in operating systems, applications, and encryption that would indicate that institutional procedures are not being followed properly. Remediate any issues uncovered.	Info: Vulnerabilities and Vulnerability Scanning	Industry
	Info: Vulnerabilities and Vulnerability Scanning	Industry

	Info: Security Self-Assessment Guide for Information Technology Systems	Industry
	Tool: Nessus	Vendor
7.4 **Routinely monitor log files of critical computing resources.** Seek out anomolous behavior. Flag changes to privileges so they can be spot-checked in mini-audits. Flag configuration changes for possible match-up to any change control process in place. Such monitoring can largely be automated.	Tool: Swatch	Other
	Tool: AWStats	Other
	Tool: Splunk (free version)	Vendor
7.5 **Routinely audit** access privileges	Info: InCommon Identity Assurance	Higher Education
	Info: Statement on Auditing Standards (SAS) No. 70	Other
7.6 **Review procurement procedures and contract language to ensure that they protect data.** Contract language is covered in Step 3.2, but it is vital to periodically check that these contracts are being consistently applied across a variety of procurement situations.		
7.7 **Implement system development methodologies** that prevent new data handling problems from being introduced into the environment	Info: Security Considerations in the Information System Development Life Cycle	Industry
7.8 **Implement incident response policies and procedures.** Even after implementing this entire blueprint, if you hold confidential data, it will be at risk, albeit at a much lower level of risk. It is wise to have procedures in place should any of this data be exposed to unauthorized parties *before* such a breach occurs, as the environment when a potential breach is discovered is fast-moving and dynamic, making it difficult to follow proper procedures if they are not already in place.	Tool: Data Incident Notification Toolkit	Higher Education
	Info: Computer Security Incident Handling Guide	Industry

#Top of page