Information Security Plan

December 21, 2012

REVISION CONTROL

Document Title:	HSU Information Security Plan
Author:	John McBrearty

Revision History

Revision Date	Revised By	Summary of Revisions	Sections Revised
7/9/2008	John McBrearty	Created Original Draft	All
11/10/2009	Mark Hendricks	Minor Modifications and Updated Priorities for '09-'10	Priorities
12/09/2009	Security Group	Reviewed by Security Group	All
	Mark Hendricks	Posted	Mark Hendricks
6/10/2010	Mark Hendricks	Updated, Policies and Standards, Risk Assessment & Mitigation, Priorities for 2010-2011	III, IV, VI
6/10/2010	Security Group	Reviewed by Information Security Group	All
5/9/11	Mark Hendricks	Updated Priorities	VI, Appendix C
5/11/11	Anna Kircher	Approved	All
5/24/11	CSIRT	Reviewed	All
12/20/12	Mark Hendricks	Updated Priorities & minor edits	VI

Introduction

In order to fulfill its mission of education and public service, Humboldt State University is committed to providing a secure yet accessible data and networking infrastructure that protects the confidentiality, availability and integrity of information.

The creation, preservation and exchange of information is an intrinsic part of the University's teaching, scholarship and administrative operations. Increasingly that information is processed, handled or stored in electronic form. The growing availability of digital information offers opportunities to improve our collaborations and work in new ways. Unfortunately, it also presents us with new threats. The very technologies we use to gather, share and analyze information also make our institution vulnerable to varied and continually evolving information security risks.

Humboldt State University is entrusted with a wide range of confidential and sensitive information pertaining to our students, faculty and staff. We take seriously our obligation to be stewards of that trust. We are obligated by law and institutional policy to take all reasonable and appropriate steps to protect the confidentiality, availability, privacy, and integrity of information in our custody. This obligation is broad and applies to information in both electronic and material form. Our practices are designed both to prevent the inappropriate disclosure of information and to preserve information in case of intentional or accidental loss.

A. Guiding Principles

The University's strategy is multi-faceted and must continue to evolve to meet an ever-changing threat. At the core, the plan is designed to uphold the following principles:

1. The University protects the *privacy of student and employee records* by ensuring the security and protection of confidential information in its custody, whether in electronic, paper, or other forms.

2. *Proper organizational structures and strategies to assure adequate controls and risk assessment are* a necessary part of protecting the privacy and confidentiality of information systems. Risk is a fact of life for any organization that must maintain the confidentiality of collected data, whether it is online or consists of paper files. Risk management must include analysis to avoid unnecessary efforts and expenses. Risk is managed on an ongoing basis, as the environment changes, new technology is released, user requirements evolve, or cost-risk factors are further analyzed. Adequate controls not only help mitigate risk but generally correspond to best business practice in assuring transparency and consistency of business processes and effectiveness and availability of underlying technologies.

3. The continuing *education and awareness* of the staff, faculty, and students on information security issues is an important factor in minimizing information security risk overall. In particular, as the University refines its guidelines and procedures for maintaining the confidentiality of information that is deemed highly sensitive, employees who handle this data need to be provided appropriate and periodic training on approved procedure.

B. Scope of the Information Security Plan

Securing our information requires a comprehensive approach. It is not sufficient to physically secure our computing hardware or software. Sound information security practice requires a combination of strategies including risk assessment, technical measures, training, and continual process improvement. Equally importantly, it requires the University community to remain informed about potential risks, mandated policies and recommended practices.

This Information Security Plan applies to all information that is acquired, transmitted, processed, stored, and/or maintained by Humboldt State University or any HSU auxiliary organization, whether in digital or paper format. It encompasses all locations in which HSU information resides including the main campus and remote campus work areas. It applies to all Humboldt State University students, employees, consultants, contractors, or any person having access to University information in any form or format.

Information Technology Services (ITS) and the campus' IT Consultants play a leading role in safeguarding the University's information security. However, information security planning and assurance cannot be successfully accomplished solely within a technical arena. This plan defines overlapping responsibilities of HSU organizational units and the intersecting responsibilities of other organizations and individuals.

C. About this Document

The remainder of this document summarizes HSU's current plan to maintain the security of its information assets. It conveys both long-term strategies and near-term activities we are pursuing to improve our overall information security environment. The plan is presented in five sections:

- Roles and Responsibilities
- Information Security Policies
- Risk Assessment and Mitigation
- Securing the HSU Technical Infrastructure
    - Priorities for Improvement This document attempts to present the plan with minimal use of technical language or specialized terms. The practice of information security is, however, evolving its own terminology in certain instances; some terms that are unfamiliar to the reader may appear in the document. Therefore, the document includes in an appendix a glossary of common information security terms.

I. Roles and Responsibilities

Currently emerging CSU-wide Information Security policies and standards require that the University muster a *coordinated approach* to the protection of information resources and repositories of confidential information that are under its custody; and that it do so by establishing appropriate and reasonable administrative, technical and physical safeguards that include all individuals, work units, or other entities that administer, install, maintain, or make use of its computing resources and other depositories of information. At HSU, that coordinated approach includes the following administrative structures and responsibilities:

The **Information Security Officer** (ISO), in formal collaboration with two levels of **Advisory Committees** described below**,** is responsible for the development, maintenance, and periodic update of this campus Information Security Plan; for the coordination and interpretation of the nascent CSU-wide Information Security policies and standards; and for the development and implementation of more specific guidelines and procedures to support those policies and standards with the particular context of HSU. Advisory Committees consist of the following:

- **The Computer Security Incident Response Team (CSIRT)**, which, in addition to responding to serious incidents, performs top level review of campus information security policies, standards, guidelines and procedures. Collectively, this group works with the ISO during the currently active development of information security policies and practices at a CSU-wide level that will apply to all the CSU campuses including Humboldt State University. This committee is also the recipient of periodic reporting by the ISO on significant security incidents and overall institutional risks and vulnerabilities.

- The **Data Managers Information Security Group**, a committee whose members primarily hold positions as data owners of record (and/or "unit custodians" as in HSU University Letter 03-03, "Student Records Access Policy," and various CSU memoranda). This committee is expected to review and discuss application-level data management and access issues to ensure that they are reasonably and consistently addressed within the University's information security technical and business guidelines, procedures and practices.

Academic and administrative managers including Vice-Presidents, Deans, Department Chairs, Directors and Managers also play an important role in the overall information security strategy. They are responsible for understanding the importance of managing information security risks both within their organizations and across the campus as a whole. They set an example and establish a tone in their organizations that stresses the importance of information security compliance and awareness. Finally, they are responsible for working with the ISO and/or their organizational IT Consultants to mitigate vulnerabilities in their areas and to collaboratively implement good information security practices.

Students, faculty and staff are all active agents in HSU's information security plan. Like the educational process itself, sound security practice benefits in both direct and indirect ways from everyone's attention and contributions. Every user of HSU technology resources and information is responsible to remain aware of information security risks, be attentive to sound practices and to report any potential disclosure or loss of information to their supervisors, instructors, or other responsible parties.

II. Information Security Policies

This section introduces the reader to the major information security legal requirements that HSU is bound to uphold and the policies the University have adopted to facilitate compliance. Detailed information on compliance requirements and policies will be coordinated with the current CSU-wide Information Security Policy development efforts and referenced on the HSU Information Security web site.

A. Compliance Requirements

HSU's information security practices must comply with a variety of federal and state laws as well as CSU's and its own campus policies. These laws and policies are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. "Level 1 protected data" as defined by the CSU covers a variety of types including personally identifiable information (e.g., social security numbers), personal financial information (e.g., credit card numbers), health information and other confidential information.

Among the laws and regulations that mandate baseline privacy and information security controls, the most notable include the following:

- **HIPAA (Health Insurance Portability and Accountability Act) -** Protective Health Information (PHI) may be used and disclosed for Treatment, Payment, and Healthcare Operations (TPO). The information that is disclosed must meet the "Minimum Necessary" standard. This means the least information required to accomplish the intended purpose. Under all other circumstances except an emergency in a patient's health, a signed authorization form must be completed by the patient or his legal representative.
- **Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. S1232g; 34 CFR Part 99) -** Protects the privacy of student education records and gives parents certain rights with respect to their children's education records.
- **Gramm-Leach-Bliley Act (GLBA) -** These requirements mandate the design, implementation, and maintenance of specific policies to protect customer information. The GLBA protects consumers' personal financial information held by financial institutions.
- **Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002 -** Implements the safeguarding provisions of the Gramm-Leach-Bliley Act. Establishes standards for safeguarding customer information and calls for the establishment by organizations of information security plans to bring about compliance.

Additional laws and regulations apply in the wake of unauthorized disclosure of individuals' data, requiring the University to take specific actions if any protected data may have been disclosed either accidentally or maliciously to unauthorized parties. A detailed list of regulations and compliance requirements is included in Appendix B. Individuals who handle protected data are encouraged to speak with their managers or the Information Security Officer to better familiarize themselves with relevant laws and regulations.

B. California State University Information Security Policy and Standards

The California State University published its Information Security Policy on April 19th, 2010. This CSU Information Security Policy is located in the Integrated CSU Administrative Manual at http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml. HSU security staff is actively engaged in drafting Information Security standards documents that prescribe methods of compliance with relevant laws and regulations as well as generally accepted current best practices. All campuses within the CSU are expected to take the further step of establishing "guidelines and procedures" with campus-wide scope, to assure that the standards inform actual practice. In June of 2010, HSU Executive Memorandum 06-2010 [10-03] HSU Implementation of the CSU Data Classification Standards was published. This Executive Memorandum implements a data classification standard that formally defines information protected due to law and privacy concerns as "level 1 protected data" requiring a higher standard of care than either routine internal communications or publicly accessible data.

The following policy areas are currently under review by the CSU.

- Information Security Roles & Responsibilities
- Risk Management
- Acceptable Use
- Personnel Security
- Privacy
- Security Awareness and Training
- Third Party Services Security
- Information Technology Security (Technical Controls)
- Configuration Management and Change Control
- Access Control
- Asset Management
- Management of Information Systems (Application Development)
- Information Security Incident Management
- Physical Security
- Business Continuity and Disaster Recovery
- Legal and Regulatory Compliance

III. Risk Assessment & Mitigation

The single most often reported types of security breaches on college campuses are those involving protected data loss. HSU, like the other CSU campuses, is participating in the rollout of a user

awareness program which commenced in fall of 2008, aimed at making all members of the campus community aware of the need to avoid storing unnecessary personal data information on workstations and storage media in their possession. Additionally, the three levels of Information Security committees at HSU will be tasked with finding practical means to reduce the campus' exposure to this preeminent form of risk.

Humboldt State University's other major Information Security risks flow from its prior lack of formal structures and consistent policies and practices relating to Information Security risk reduction. Those issues are being addressed across the board through the new committee structures and CSU-initiated policy and standards development discussed elsewhere in this document.

Our information security risk reduction plan will be further enabled by three core practices:

- risk assessment
- incident response
- employee education and training

These practices will enable us to proactively identify risks, continuously improve our strategy and direct our response in case of an information security incident. This section briefly describes HSU's current or planned approach to each core practice. Additional information can be obtained from the ISO and will be incorporated in the future on the campus' information security web site.

A. Risk Assessment

HSU will perform periodic assessments of its information security risks and vulnerabilities. Risk assessments may be aimed at particular types of information, areas of the organization or technologies. Each year the ISO in consultation with CSIRT committee will identify a set of priorities for risk assessments.

Each risk assessment includes, at a minimum, the following elements:

1. A list of assets in the business environment
2. A determination of the information security needs of the university computers and networks
3. An evaluation of the management and control of information security risk including:
    a. A list of relevant threats
    b. An evaluation of probability and impact for threats
    c. Mitigation strategies for key risks
4. Feedback and remediation strategies including staff orientation and training

The results of risk assessments will be shared with the CSIRT committee and the Executive Committee. They will include a plan for implementing specific actions to address risks and vulnerabilities. The ISO will be responsible for monitoring the implementation of agreed upon actions and reporting their completion to University leadership.

In the long-term, the ISO will seek to create a risk assessment capability within the information security organization that can proactively perform risk assessment at the request of individual university departments.

B. Managing compromises or breaches of information security – Incident Response Team

Planning for incident management involves organizing an Incident Response Team that is responsible for *problem identification and resolution*. This team has clearly defined membership, roles, and responsibilities. The issues an Incident Response Team is concerned with include (but are not limited to):

1. Incident Management
    a. How to trigger a response
    b. Automated and manual responses
    c. Reporting responsibilities
    d. Certification of actions
    e. Post-Incident review and recommendations
2. Existing and Evolving Threats
3. Information Security Testing

Notification of a significant security incident begins after the reporting of a security related event at one of several possible locations within Humboldt State University, such as the ITS help desk, the Information Security office, one of the standard incident-reporting University email addresses, or the University Police. When an alert involves personally identifiable information and/or appears to be a serious or potentially public incident, the cross-functional CSIRT team composed of members from different areas of the University will respond following the University's best practice incident response procedures. The core members of the Computer Security Incident Response Team (CSIRT) are the following:

- Risk Manager
- Chief, UPD
- Special Assistant to the President
- Chief Information Officer

- Senior Communications Officer
- Information Security Officer, Chair

In addition, the following managers are to be included as part of the standing CSIRT group at their discretion to discuss topics of concern to them, and also as a key resource when a serious or potentially public incident includes likely culpable participation by students, staff or faculty, respectively:

- Student Conduct Administrator
- Associate Vice President, Human Resources & Accounting
- Associate Vice President, Faculty Affairs

C. Employee Education and Training

The entire University Community needs to understand and support the information security objectives of availability, confidentiality and integrity, and what tradeoffs may be necessary for effective control of the information infrastructure's vulnerabilities. The California State University has established an online information security awareness program to serve all 23 campuses that will promote an ongoing dialogue about information security risks and recommended practices. All staff, faculty, and student staff have been enrolled in this training.

HSU has a multi-pronged approach to training and awareness. Current strategies include the following:

- A privacy and confidentiality agreement to be signed by all newly hired staff
- An online CSU Information Security Awareness Training course for all staff, faculty, and student staff
- An information security website that serves as a repository of information for HSU information security standards and its Appropriate Use Policy as well as additional information about current issues, policies and practices
- Periodic communiqués to the University community alerting HSU students and employees to specific vulnerabilities
- Specific training for campus personnel with information security responsibilities

D. Personally Identifiable Information (PII Inventory)

HSU Executive Memorandum 06-2010 [10-03] HSU Implementation of the CSU Data Classification Standards establishes standards for the classification of data types. In addition to defining these standards, the Executive Memorandum requires that protected "Level 1" and "Level 2" data be located on campus computers and removed unless a valid business function exists and the storage of this information is approved by the HSU President or designee. In the Fall of 2010, all campus workstations were scanned for protected data. This scan or "survey" was used to create an inventory of sensitive data. In 2011 a second scan of campus workstations was conducted, targeting positions where large volumes of PII had previously been located. The goal of this scan was to identify business processes that were propagating PII. In 2012, server scans were conducted to identify, delete, or protect PII stored on file servers.

IV.Securing the HSU Technical Infrastructure

This section identifies some of the specific strategies in place to secure the core technology infrastructure (e.g., network, hardware, data center) of the University. It describes some of information security concerns unique to specific technology areas and highlights the measures being employed to secure HSU infrastructure.

A. Networking Environment (data, video, and voice)

Among the concerns at HSU for network and operations security are assurance of service, spam rejection, copyright protection, appropriate authorization for the use of resources, privacy/confidentiality, protection against unauthorized network access, protecting web sites from typical attacks, and maintaining auditable documentation of plans and procedures. The following technologies and tools supported by the appropriate policies and procedures are implemented to address these needs:

- Firewall, Traffic Monitoring and Notifications Response
- Virtual Private Network
- Campus-wide Authentication Service
- Limiting Physical Access to Servers and Other Resources
- Email Encryption and Campus-wide Email Upgrade
- Organization of Staffing to Respond to the Range of Security Issues

B. Enterprise Server Environment

Deployment of a managed server facility protects the enterprise servers from unauthorized access and assures appropriate logging, archiving and monitoring. Operational procedures allow physical access only to authorized users and helps ensure that all other staff access servers only to the degree appropriate to their job roles.

C. Identity and Access Management

HSU's overarching identity management and authentication resource ensures appropriate limits on access to all campus computing resources. Network and server access is logged by individual logins to facilitate investigation of possible intrusions or misuse of resources. For applications, only the minimum set of privileges allowed for a user to accomplish his/her objective is granted.

V. Priorities for Action – 2012-2013

This HSU information security plan will be regularly updated and modified. For the 2012-2013 academic year, the information security priorities of the University include:

Continue collaboration with system-wide groups

- Information Security Advisory Committee (ISAC)
- Virtual Information Security Center (VISC)
- Identity and Access Management Technical Architecture Group (IAM-TAG)
- CSU Infrastructure Advisory Group

Information Security and Awareness training program

- Implement Information Security training program
- Participate with system-wide awareness training RFP
- Deploy mandatory security awareness training
- Secure Programming Support (OWASP)

Complete and maintain protected information asset management

- Conduct Server PII Scans to complement workstations scans
- File Encryption for Level 1 data
- Identify physical areas that work with sensitive data
- Labeling of sensitive data

Registry and Password Management Project

- Extend and improve ARF process
- Automation of employment change access review
    - remove security roles and group access with employment change
- Investigate requirements for InCommon Silver

Mobile Device Security

- Develop support for Mobile Devices/BYOD
- Controls Mobile Devices: 8045.400

Managing 3rd Parties 8040.100 & 200

- Implement Information Security contract language review
- Participate in software selection process

Appendix A: Glossary of Terms

Attacks are deliberate actions taken by an entity that exploit certain vulnerabilities.

Authoritative Decision Maker is the person who made the decision regarding compliance in the referenced section.

Availability is a property that assures that the system has the capacity to meet service needs. It includes timeliness and usability. The property of availability protects against threats of denial of service.

Controls are mechanisms or procedures that mitigate threats. Among the goals of information security controls are to provide confidentiality, integrity, availability, or privacy to a computer system.

Confidentiality is a property that assures the assets of a computer system are accessible only by authorized parties or entities. The property of confidentiality protects a system from the threat of disclosure. A disclosure threat is the possibility that data will be accessed by unauthorized entities.

Consultants are experts hired by the university to provide assistance with its information systems or other activities.

Contracted service providers are third parties including businesses that are hired by the University to provide assistance with the information systems infrastructure.

Integrity is a property that assures that unauthorized changes in data cannot occur or can be detected if they do occur. The property of integrity protects against threats of modification and fabrication.

Privacy is a subset of confidentiality. It concerns data about an entity and assures that this data is not made public or is accessible by unauthorized individuals.

Risk analysis is the study of the consequences involved in doing something or not doing it. It improves the basis for information security related decisions and helps justify expenditures for information security.

Threats are potential occurrences, malicious or otherwise, that can have undesirable effects on assets or resources associated with computer systems.

Vulnerabilities are characteristics of computer systems that make it possible for a threat to potentially occur. They are not necessarily weaknesses in a system and may be otherwise desirable qualities of a system.

Appendix B: Regulatory Compliance Requirements

Regulation	Summary
Family Educational Rights and Privacy Act (FERPA)(20 U.S.C. S1232g; 34 CFR Part 99)	This protects the privacy of student education records and gives parents certain rights to their children's education records.
California State Constitution, Article 1, Section 1	This is a general description of the rights of citizens in California.
California Penal Code, Section 502	This defines the criminality and responsibility for specific computing activities and associated punishments.
Gramm-Leach-Bliley Act	GLBA requirements mandate the design, implementation, and maintenance of specific policies to protect customer financial information.
Federal Trade Commission Regulations (16 CFR, Part 314), Standards for Safeguarding Customer Information; Final Rule, May 23, 2002	This establishes standards for safeguarding customer information and creates a method to guarantee the uniform application of these standards.
California Business and Professions Code Section 17538.45	This protects electronic mail providers from liability and provides them with a remedy in the event of unauthorized use of email functionality.
State of California Government Code, Section 11015.5	This law pertains to the confidentiality of electronically collected personal information.
California Information Practices Act of 1977	This act gives specific direction on how to handle personal information and describes the right to privacy of individuals.
State of California Government Code, 6254 (j), 6254.4, 6255, 6267	These laws govern the privacy of library users' records.