Information Technology Council
Humboldt State University

Meeting Notes for: March 11, 2008 from 2:00 to 4:00 P.M., NHE 106

Members Present: Mark Hendricks (Chair), Dave Marshall (CNRS), Steve Darnall (CAHSS – proxy for Megan McKenzie), (Jeanne Wielgus (DITSS), Rick Garcia (TNS), Greg Osburn (OEM – proxy for Dale Sanford), Drew Meyer (Housing),), Cassandra Tex (SDRC), John McBrearty (ISO), Dave Pearson (CPS), Toby Walker (SA), Tera Mar (OAA)

Others Present: Bugs Brouillard (CITSS-UCS), Ed Gordon (CNRS), Josh Callahan (CITSS), Shawn Kohrman (DITSS), David Peters (AF), Anna Kircher (CIO), Molly Simpson (Recorder).

1. Approval of the Minutes:

February 2008 Minutes were approved as distributed (McBrearty/Marshall)

2. Report Items:

DSWAG: Darnall reviewed the minutes of the February 21, 2008 DSWAG meeting. He noted that the group was requesting a charge from the IT Council to develop a plan for coordination of OS migrations.

A motion was made for the IT Council to charge DSWAG with developing a plan to coordinate OS Migration; this motion was followed by a friendly amendment requesting that reasoning be included in the plan. The motion carried (McBrearty/Wielgus).

Darnall informed the council that Hendricks agreed to create an HSU procedure based on the centralized authorization memo that McBrearty presented to the council in February. Darnall stated that the draft would be presented to the IT Council for review in April.

Lab Stats (currently being used in the interdisciplinary labs) is now available to other areas of campus if they wish to buy-in. Sample reports will be available for review, and interested parties should contact Josh Callahan and cc Molly Simpson for details on the buy-in and server access.

Network folders are being tested in several labs with overall stable results. Darnall reported that Desktop IT will soon be testing the use of network folders in smart classrooms. Hendricks noted that network folders were ready to go into the final testing stage and that ITCs should encourage their advanced users to test the network folders. The next phase will be to present the campus with information - April 21st.

Darnall asked Council members to review the list of voting DSWAG members (on back of DSWAG handout) and report additions or deletions to him.

3. Discussion Items/ Action Items:

Monthly Service Window: Callahan told the Council that he and Paul Picciotta were in the process of authoring procedures for change management of enterprise systems. He noted that he would put the draft document on Moodle for feedback. Callahan - indicated that a change control group might be started as a part of the change management process. Callahan informed the council that the service window would be a standing agenda to better communicate service windows events. Hendricks noted that normal patches would be applied during the March Service Window; however, Telecommunications had a busy schedule and would require a longer window. Garcia requested that the Service Window be changed to 3:00 A.M. to 6:00 A.M to allow TNS time to migrate mission critical systems to the new switch, separate infrastructure. Service windows are scheduled for April 19th and again on April 26th if needed for these core upgrades.

Update on Information Security Policy and Standards Implementation: McBrearty reviewed the status of the CSU System-wide Information Security Policy and Standards rollout. He noted that the "Policies and Standards" represent the top level of information security rules and will be reviewed and implemented across the board for all 23 campuses. More specific "Guidelines and Procedures" will be then developed by each campus. Currently a second draft of the System-wide Policy document is expected soon, along with the initial draft document for Standards. McBrearty will share draft documents with the ITCs as they become available to him. It is expected that the Policy and Standards adoption process will be complete around the end of summer 2008.

McBrearty also distributed the campus' draft Information Security Plan, which specifies the coordinating role of three committees, one of which is the IT Council. He asked for any comments or feedback by next meeting.

McBrearty mentioned that the CSU Office of the University Auditor will be doing an Information Security subject-matter audit at each of the campuses over the next year and a half. He will be presenting information including checklists of materials needed for the audit at upcoming IT Council meetings.

Lastly McBrearty noted that an RFP has been issued by the CSU for an on-line information security awareness training program. There may be some concrete results in place from that as early as this summer.

DITSS Vista Deployment Postponement: Kohrman announced that the roll-out of Vista to campus labs would be postponed for one year.

ITRP2 (core upgrades, equipment refresh, wireless): Garcia informed the council of several large projects that would be occurring over the next several months. In April two service windows would be required to allow AT&T engineers to re-program the campus Core switch/routers to meet current CSU configuration standards. Garcia also indicated that another CSU project starting shortly would refresh switch equipment across campus, and yet another project would begin the ITRP2 wireless implementation at Humboldt.

ATI Training Update: Quarles reviewed the ATI training model noting that those requesting accounts on new server would be required to complete one or more ATI trainings. Quarles update the Council concerning the development of a questionnaire that individuals would complete that would determine which training(s) they would be required to complete. Some training will be in Moodle and some will be face to face training either live or recorded. Quarles reviewed compliance dates reflected in the ATI coded memorandum.

Network Folders Update: covered under DSWAG report.

Mail Replacement Update: Callahan reported that after a long and thorough review process, it was determined that Zimbra would be the best fit for the HSU Campus. Some funding and some savings from other licenses will allow us to purchase the Zimbra license and testing should begin this spring. Work is in progress to come up with an informational campaign. The campaign would combine other projects as well.

Adjournment: (Shellhase/Marshall) 3:05 P.M.

IT Council Agenda

Next Meeting: Tuesday, March 11th, 2008 *Location: Nelson Hall East Room 106 Time: 2:00 P.M.*

I. Approval of the Minutes

http://www.humboldt.edu/~its/planning/committees/itcpdf/ITC021208.pdf

II. Working Group Report Items

1. DSWAG: Darnall

III. Discussion Items/Action Items

1. Monthly Service Window: Callahan 2. Update on Information Security policies and standards implementation: McBrearty

IV. New Business

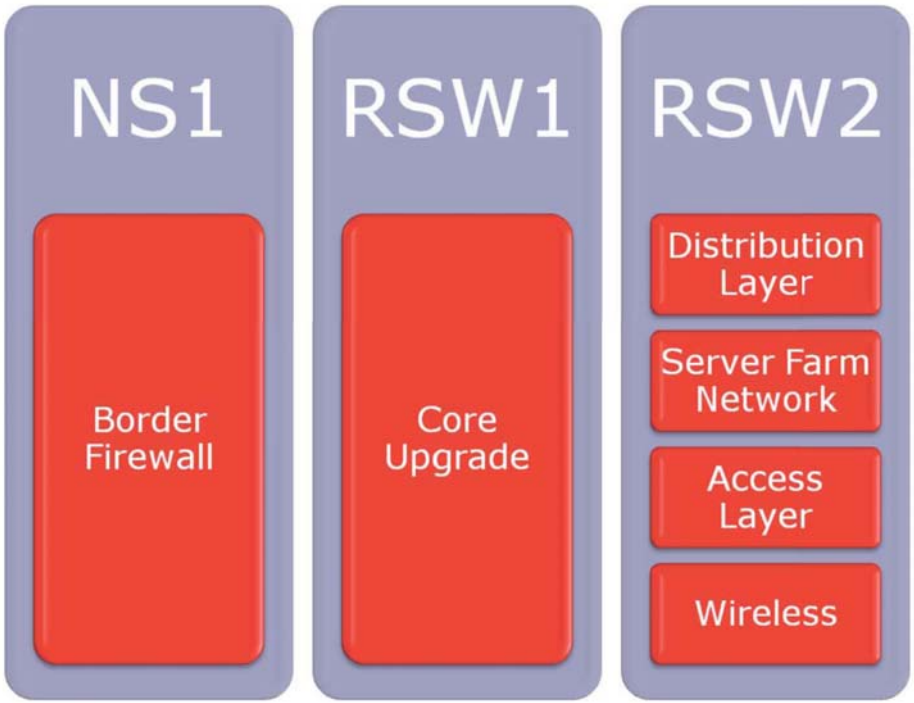
1. 1. DITSS Vista Deployment postponement: Kohrman
2. 2. ITRP2 (core upgrades, equipment refresh, wireless): Garcia
3. 3. ATI Training update: Quarles
4. 4. Network Folders Update: Hendricks
5. 5. Mail Replacement Update: Callahan

V. Announcements

Apple visit

VI. Adjournment

Program


NS1
Border Firewall
RSW1
Core Upgrade
RSW2
Distribution Layer
Server Farm Network
Access Layer
Wireless

Name	Organization	Email
Wielgus, Jeanne	Desktop Support (Labs)	jw7001@humboldt.edu
Walker, Toby A	Student Affairs	taw2@humboldt.edu
Pearson, David	CPS	david.pearson@humboldt.edu
Osburn, Gregory N	Enrollment Mgt	gno2@humboldt.edu
McBrearty, John	ITS -ISO	jm145@humboldt.edu
Marshall, David	CNRS	dem1@humboldt.edu
Hendricks, Mark D	Central IT	mdh3@humboldt.edu
Gilden, Bethany L	Desk Support Coordinator	blg10@humboldt.edu
Darnall, William S	CAHSS	wsd1@humboldt.edu

DSWAG Meeting on Feb. 21, 2008

1. Campus Wide OS standards/support
    - Resolution was passed to request a charge from the IT Council to develop a plan for coordinating OS migrations. The purpose is for articulation and preparation, not the creation of mandates. The formality is so that ITCs can approach their respective administrators with schedules and requests for resources based on an implementation calendar (guideline?) developed by DSWAG. This is not meant to restrict the OS choices for every system on campus. We recognize that there are new Vista systems that will not run XP, and existing systems that are not compatible with Vista or Mac OS 10.5. A coordinated plan is necessary to present users similar environments in computer labs.

2. Development of a procedure regarding user authorization and anonymous accounts.
    - Mark Hendricks has agreed to create a draft of this procedure for review at the next meeting.

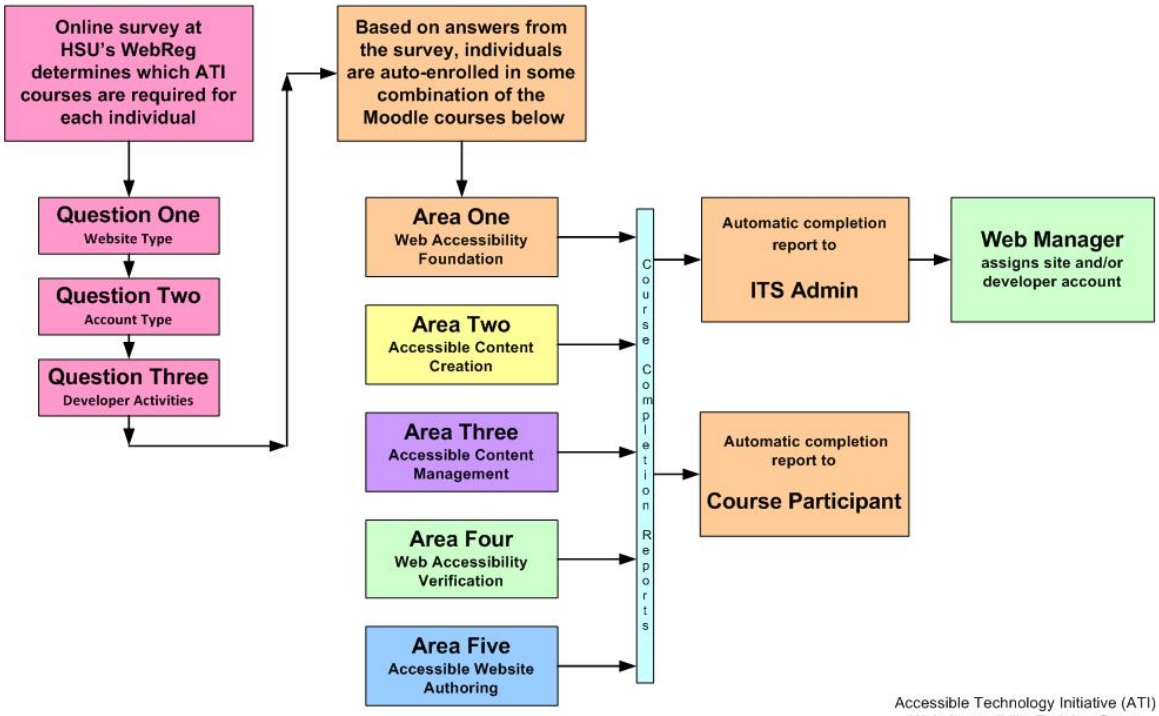
3. Lab Stats
    - John Adorador will ask Anna Kircher for approval of using one of their reports as an example for those interested.
    - Contact Josh Callahan (cc Molly Simpson) for details on the buy in and server access.

4. Network Folders
    - \\folders.humboldt.edu\faculty and \\folders.humboldt.edu\<user id> are being tried in various OUs with overall stable results. Desktop IT will soon be testing their use in smart classrooms. A firm date has not been set for going public.

(This following is included since it was in the summation emailed to DSWAG members; the final arrangements of the visit were with the parties interested in Leopard server and OD/AD configurations)

5. Apple tech coming to campus regarding Open Directory.
    - The Tech's name is Mark Johnson; his latest email suggested 8-9:30 am on Tuesday March 11. Those interested were requested to email wsd1@humboldt.edu with presentation suggestions ASAP so we could communicate our expectations to Mr. Johnson before confirming the visit.

Process for defining individual workshop training responsibilities



Accessible Technology Initiative (ATI)
Web Accessibility Training Group
Revised 03.07.08

Information Security Plan

version 0.1 (DRAFT)

March 10, 2008

Prepared By:

John McBrearty
Information Security Officer
Humboldt State University

I. 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.

Much of our teaching, scholarship and administrative operations depend on the creation, preservation and exchange of information. Increasingly that information is processed, handled or stored in electronic form. The growing availability of digital information offers tremendous 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 (HSU) 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 good stewards of this 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. Our 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

Our 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 evolves, new technology is released, user requirements change, or economic conditions fluctuate. Adequate controls not only help mitigate risk but generally correspond to best business practice in assuring transparency and consistency of key business processes.

3) The continuing *education* of the staff, faculty, and students on information security issues is a large part of information security in a University. In addition, as the University refines its guidelines and procedures for protecting the confidentiality of sensitive information, employees who handle this data need to be appropriately trained on these updated procedures.

B. Scope of the Information Security Plan

Securing our information requires a comprehensive approach. It is not sufficient to merely secure our computing hardware or software. Sound information security practice requires a combination of strategies including risk assessment, technical measures, training, and continual business process improvement. Equally importantly, it requires the University community to remain informed and vigilant about risks, 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 various 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 recurring strategies as well as the near term priorities we are pursuing to continuously improve our overall information security environment. The plan is presented in five sections:

- Roles and Responsibilities
- Security Policies
- Information Security Practices

- Securing the HSU Technical Infrastructure
- Priorities for Improvement 2008 - 2009

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.

II. Roles and Responsibilities

The University assumes a *coordinated approach* to the protection of information resources and repositories of confidential information that are under its custody 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 HSU's computing resources and other depositories of information.

The **Information Security Officer** (ISO) is responsible for the development, maintenance, and periodic update of the Information Security Plan, in collaboration with three levels of advisory committees:

- **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, these individuals oversee the development and implementation of policies and practices that maintain our information security. They are also the recipients of periodic review of institutional risks and vulnerabilities.
- A **Data Managers Information Security Group**, a new committee whose exact composition will be ratified by the CSIRT team, is expected to be convened beginning Spring 2008 to review and discuss general data management issues to ensure that they are reasonably and consistently addressed within the University's information security framework.
- The **Information Technology Council**, a existing campus group comprised of campus IT Consultants as well as Information Technology Services area managers, meets monthly and will be expected to offer input and consideration especially of the technical aspects of information security policies and procedures.

Academic and administrative managers including Vice-Presidents, Deans, Department Chairs, Directors and Managers also play a pivotal role in the overall information security strategy. They are responsible for understanding the overall information security plan. They establish a tone in their organizations that stresses the importance of information security awareness and sound practice. Finally, they are responsible for working with the ISO to identify vulnerabilities in their areas and to implement reasonable measures to counter threats.

Students, faculty and staff are all participants in HSU's information security plan. Like the proverbial chain, our information security practices can only be as strong as our weakest link. Every user of HSU technology resources and information is responsible to remain aware of information security risks, seek training in sound practices and to report any potential disclosure or loss of information to unauthorized parties.

III. Information Security Policies

This section introduces the reader to the major information security requirements that HSU is bound to uphold and the policies the University has 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 policies. These regulations are generally designed to protect individuals and organizations against the unauthorized disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information including personally identifiable information (e.g., social security number), personal financial information (e.g., credit card numbers), health information and confidential student information.

There are many individual laws and policies that establish our information security requirements. Some of the most notable include:

- **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 regulate the disclosure of employee and student data and require the University to take specific actions in the event HSU suspects that 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 ISO to better familiarize themselves with relevant laws and regulations.

B. University Information Security Policies

The California State University is developing a body of information security policies that prescribe methods of compliance with relevant laws and regulations. Humboldt State University, like the other local campuses within the CSU, will be required to take the further step of establishing guidelines, procedures and practices to safeguard not only information protected by law, but also information that CSU leadership has deemed to be of a sufficiently confidential nature that it should be treated as legal protected data.

The following policy areas are currently under review by the CSU. Their adoption is anticipated by means of a Chancellor's Office coded memorandum during fiscal year 2008-2009:

- Information Security Roles & Responsibilities

- IT Security (Technical Controls)
- Access Control
- Third Party Services Security
- Personnel Security
- Business Continuity and Disaster Recovery
- Risk Management
- Security Awareness and Training
- Security Incident Response
- Managing Information Systems
- Privacy
- Acceptable Use
- Asset Management
- Legal and Regulatory Compliance
- Information System Logging & Monitoring
- Physical and Environmental Security

IV. Information Security Practices

Our information security plan is further enabled by three core practices:

- risk assessment
- incident response
- employee education and training

These practices 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 approach to each core practice. Additional information can be obtained from the ISO or the 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. An inventory of information 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. Risk assessment
    b. Mitigation of risk
    c. Vulnerability assessment
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.

During calendar year 2008, HSU's risk assessment will be coordinated with an anticipated campus-level Information Security Audit to be conducted by the Office of the University Auditor at all 23 campuses including Humboldt.

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):

a) 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

b) Existing and Evolving Threats

c) 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 comprised 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:

1. Risk Manager (Dave Bugbee)
2. Chief, UPD (Tom Dewey)
3. Special Assistant to the President (Denice Helwig)
4. Chief Information Officer (Anna Kircher)
5. Senior Communications Officer (Paul Mann)
6. Information Security Officer (John McBrearty), 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:

7. Student Conduct Administrator (Randi Darnall Burke)
8. Director, HR (Tammy Curtis)
9. Associate Vice President, Faculty Affairs (Colleen Mullery)

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 issued an RFP for on on-line information security education program to serve all 23 campuses that will promote an on-going dialogue about information security risks and recommended practices.

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 information security website that serves as a repository of information for HSU information security standards and its Appropriate Usage 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

V. 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)

The primary concerns at HSU for network and operations security are in the areas of assurance of service, spam rejection, copyright protection, appropriate authorization for the use of resources, privacy/confidentiality, and protection of physical assets. 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.

VI. Priorities for Action – 2008 - 2009

This HSU information security plan will be regularly updated and modified. For the 2008-2009 fiscal year, the information security priorities of the University include:

- Developing an appropriate organizational structure to provide a unified framework of authority for the campus' Information Security policy and enforcement efforts
- Coordinating with the CSU system-wide rollout of Information Security Policies and Standards
- Preparing for the campus level Information Security audit from the CSU Auditor's Office
- Coordinating the expected CUS on-line Security Awareness Training program among various groups across the campus
- Enhancing and vetting a fully functioning Computer Security and Incident Response framework
- Defining the campus' data classification standards and encouraging the adoption of measures to abate the maintaining of protected data on desktop and laptop devices

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.

Regulation	Summary
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.
California Education Code 89546, Employee Access to Information Pertaining to Themselves	This summarizes an employee’s rights to review his or her employment records.
HIPAA (Health Insurance Portability and Accountability Act)	This describes the protection for Health records and accountability for its disclosure.