Information Technology Council
Humboldt State University

Meeting Notes for: August 12, 2008 from 2:00 to 4:00 P.M., NHE 106

Members Present: Mark Hendricks (Chair), Dave Pearson (CPS), Megan McKenzie (CAHSS), Greg Osburn (OEM – proxy for Dale Sanford), John Filce (OAA), Dave Peters (BIS – proxy for Dave Rowe), Cassandra Tex (SDRC), Rick Garcia (TNS), John McBrearty (ISO), Jeremy Shellhase (Library), Jeanne Wielgus (DITSS)

Others Present: Anna Kircher (CIO), Shawn Kohrman (DITSS), Josh Callahan (CITSS), Lorrie Marsh (TNS), Mike Bradley (CITSS), Steve Darnall (CAHSS), Bugs Brouillard (CITSS), Scott Ventuleth (TNS), Bethany Rizzardi (DITSS), Molly Simpson (Recorder)

1. Approval of the Minutes:

May 13, 2008 minutes were approved as distributed.
June 10, 2008 minutes were approved as distributed.

2. Report Items:

DSWAG: Skip – this will be covered in section 3.

3. Discussion Items/ Action Items:

Monthly Service Window: Hendricks informed the Council that the next service window would be Sunday, August 17th from 5:00 A.M. to 11:00 A.M. All major services will be affected. Systat notification will be sent out prior to the outage.

Wireless Service Pack Requirements: Hendricks reminded the Council that our current procedure requires patch updates every three months; however there have been issues with Service Pack III (PS3). Discussion ensued regarding updates. ITS has no control over updates that are labeled critical. SP3 is not labeled as such at this time. McBrearty made a motion not to require SP3 until mid fall. The motion carried (McBrearty/Pearson).

Password Aging: Callahan reported that all staff would be required to change their password every 4 months. This schedule is required to support Peoplesoft Student access. More information will be communicated to campus; however, Callahan wanted to inform ITCs in advance. Interest in extending this over to CMS Finance was noted.

CSA XP SP3: Already covered.

ITRP Network Baseline Architecture Document: Garcia announced that the AGM circuit would be down for an hour on August 18th, but would not affect services. The following documents are available for review:

- ITRP Network Baseline Architecture
- Network Infrastructure Requirements and GAAP Report
- ITRP2 Refresh (Prelim info)

Garcia will email the link to the ITC listserv.

ITRP2 Refresh: Garcia reported that as part of the refresh the Chancellor's Office will be replacing existing network equipment.. The work will be done during normal business hours unless the campus wants to fund the off hours charges. If done during normal business hours, there will be outages.

Garcia told the Council that there had been some recent port security violations. TNS will be producing a list of names associated with the violations and passing it on to the appropriate ITC, Deans, and Chairs.. The ITC can work with the end users to explain the issues and resolve.

ITRP Wireless Project: Ventuleth updated the Council on the ITRP wireless project noting that installation of new access points will begin next semester. The project is currently in the planning stage. TNS is in the process of installing jacks for the new equipment. Once all of the jacks are installed the Chancellor's Office will send 100 wireless access points at a time. The project will be done in phases. The Library will be one of the first areas. The project is moving quickly. The new equipment will have additional features that will allow for more secure wireless transmission based on roles. McBrearty made a motion to reinstate the Network Advisory Group (NAG) and charge them with reviewing the wireless rollout. The motion was carried (McBrearty/Garcia).

WSUS Server: tabled

Zimbra Rollout: Rizzardi review the following documents:

- Email Client Comparison
- Zimbra Details for End Users (document revised and replaced at meeting)
- Zimbra Details for ITCs.

Rizzardi noted that DITSS would have a table out on the quad the first week of school to distribute information about Zimbra to the campus. The rollout date is scheduled for October 20th, 2008. At this point old clients such as Outlook and Eurdora will still work. The email comparison document will help ITCs and end users determine what Zimbra client to choose.

She stated that users will have to be responsible for moving their calendar data (meetings) over to Zimbra. MeetingMaker will still be available off line for historical data only. Discussion ensued regarding archiving email from old clients and document retention rules that will be in place in the near future. Rizzardi and Filce plan to create a how to guide with FAQ to help with the archiving process.

Email quotas with Zimbra will be 500 MB (for faculty and staff) and users should be encouraged to use network folders as much as possible. Some areas may have users that have special circumstances that require them to have a higher quota. If the list is not too long we may be able to accommodate. ITCs agreed to forward a list of these users to Callahan for review.

CSU Information Security Audit Preparations: McBrearty informed the Council that the spreadsheet he is distributing at this meeting, comprising of the Office of University Auditor's Request for Documents list plus HSU's notes, will be available on the ITC123 Moodle site under "ITC Documents" in a topic labeled "Humboldt's response to CSU's information security audit requests." The Auditor's list of items for the KPMG technical portion of the audit will also be placed there. In addition, responsive audit documents will be made available under folders in that section, grouped by item number, as they are received by him.

The security audit has engaged eight campuses this year with two campuses remaining for 2008. Humboldt could be one of the two remaining campuses to be audited this year. If not, the campus will be audited in 2009. McBrearty will also post selected documents from Fullerton's audit, which they have generously shared with the other campuses, under the same folders by item numbers, if they appear useful and after he has sanitized them as necessary.

The audit is also asking for a list of all software site licenses on campus. Simpson has forwarded a list of the licenses handled through ITS; however, ITCs should submit information on any site licenses handled through their areas. The list should include vendor, product, and coverage period. More detail may be requested later.

McBrearty went through the different main categories of the Auditor's document request:

- Security Policy
- Information Security Organization (org charts, chain of command, job descriptions)
- Asset Management
- Human Recourses Security
- Operations Management

- Access Controls (individual approval of staff access by data custodians, documentation of AD Group Polices)
- Incident Response
- Compliance – legal (PCI auditing procedures)
- Web Development (still need to pin this down on the campus)

Some important tasks, such as documenting all credit card acceptances by the campus and assuring Payment Card Industry (PCI) compliance, cut across a number of categories such as Organization, Asset Management, Access Control and Compliance.

McBrearty also distributed the document list for the KPMG technical portion of the audit, noting that the campus firewall rule set must be aligned to the principle of "default deny" as soon as it is reasonably possible in order to conform to accepted security standards. He is proposing a target date between November 1-15. The change means that unsolicited requests for services from the outside will be rejected if they have not been documented and approved. This should not be any problem for the campus' known web servers, for example. But if someone's workstation is acting as a FTP server, outside campus access to that would be blocked, absent further documentation and approval.

Secure disposal of Media: McBrearty informed the Council that secure data items that had a request for disposal were being picked up today. Moving forward ITCs may be asked to document their disposed secure media using a specific format, as more specific standards are developed..

4. New Business: none

5. Announcements:

Rizzardi announced that Resource 25, the scheduling tool, will require end users (ASCs) to update the Oracle client on their computer. This will happen sometime in November. A memo informing campus will be sent by the Office of the Registrar or Information Technology Services.

6. Adjournment: (Tex/Pearson) 3:45 P.M.

DSWAG August 5, 2008 Meeting Summary

1. Zimbra migration discussion

   Please see Rizzardi documents

2. Network Folders

   The folders are being used (tested?) by various entities; mostly in the Colleges. Vista SP1 and subsequent updates appear to change the LAN Manager Authentication level to "Send NTLM response only." Check this setting if mounting network folders fails on a Vista machine. The automatic mounting with logon scripts has not correctly worked in Vista since SP1. Mounts in the other operating systems are working at this time. Leopard requires an extra password entry and there is an issue with defaulting to common names instead of HSU user names; so using a script is recommended.

3. XP-SP3 deployment discussion
   a. Installation effects of which to be aware:
      Changes some firewall settings, mostly it sets the scope to subnet.
      Device drivers may need to be reinstalled, mostly on older notebooks.
      May need to update management software and reconfigure wireless settings

   b. It was requested that CSA not require SP3 until ITCs and users have an opportunity for remediation. This will need to be brought up in IT Council.

   c. Josh Callahan will be looking into setting up a software update server.

Email and Calendar changes coming soon!

HSU has had the same email system for over 15 years, and used MeetingMaker for over 10 years. Things have changed in the email and calendaring worlds, and it's time for HSU to change, too! We are pleased to announce that we are ready to replace HSU's email AND calendaring systems!

Beginning October 20, 2008, Zimbra will be available to campus to use for both their email and calendaring needs. Zimbra combines mail and calendar into one easy-to-use interface that's the same whether you are on campus or traveling the world. Zimbra lets you share a mailbox or calendar with any other HSU user, and you can look up HSU email addresses right from within your email message. Zimbra also offers a new set of features called "Collaboration Tools" that will make it easy for groups (students, staff and faculty alike) to work on common documents together.

An Important Point to Understand about Email

Email systems are comprised of two basic components; (1) the server software that knows how to receive, route, and store emails for the whole university, and (2) the client software (like Eudora or Outlook) that lives on your computer and knows how to gather and present your emails to you. HSU will be using the Zimbra server software as its university email database, but you have several choices about what client software you use on your computer.

How Do I Know Which Email Client to Choose?

We heartily recommend that everyone use the "Zimbra Web Interface" (Windows, Mac and Linux users alike) to enjoy the best email experience. You'll be able to use the same interface whether you are on or off campus, your email and contacts will look the same no matter where you are, and your calendar will appear in the same application as your email.

UNLESS
you frequently rely on "off-line" mode for reading and replying to your email (e.g., you read and reply to emails on airplanes, or other locations where you don't have any internet connectivity). Then, you might want to consider the "Zimbra Desktop Client" which provides the same functionality as the Zimbra Web Client, *plus* the ability to synchronize your email and calendar before and after you perform off-line work. This client requires a small amount of configuration to work properly, so you may want assistance from an ITC to ensure it is set up properly.

OR
you just love Outlook or Mail or some other client and don't have the spare energy right now to learn how to use the Zimbra Web Interface. (But we really think you'll love the Zimbra Web Interface! Come on - TRY it! ☺)

Be aware that there may be some limitations with using these other clients - mostly the ability to look up email addresses while composing a new email message, or view other users' free/busy times on their calendars. (See www.humboldt.edu/~its/techguides/zimbra/compare.shtml for more details)

We hope you'll try the Zimbra Web Client - we think you'll love it!

What help can I expect?

Once Zimbra is available (October 20, 2008), IT staff will visit your office to help you move to the Zimbra Web Client. It may take some time to get to everyone's office, but you can expect your ITC to schedule a time with you.

Moving your mail

If your mail is stored on the server (IMAP or webmail users), it will be automatically moved to the Zimbra server for you. If you download all of your mail to your computer (POP users), IT staff will help you move that mail to the Zimbra server.

Moving your contacts

IT staff will be able to help you move your address book contacts to the new server during their visit to your office.

Moving your calendar items

Unfortunately, there is no good automated tool that will successfully move all your appointments from MeetingMaker into the Zimbra calendar, so you will need to manually move your appointments. The Zimbra calendar will be available for you to start populating on October 6th. You should re-schedule any meetings that you initiated and accept invitations from others as they come in. Meeting room accounts (e.g., BSS 508) will be automatically created, but their schedules will have to be re-created. During these two weeks, you will be keeping two calendars up to date.

Training

Classes will be offered beginning October 6th.You will be able to sign up for classes by going to www.humboldt.edu/~ftsc.

"How To" guides

Zimbra's Help menu provides detailed instructions for most common tasks. If you run into a problem that the Help menu does not cover, contact the Help Desk at 826-4357.

Where to call

For general Zimbra questions, contact the Help Desk at 826-4357. If you need advice about which client to choose for your office computer, you should contact your ITC.

Important Dates

10/6 .....Start moving your calendar events to Zimbra

10/6 ..... Zimbra training classes begin

10/20.....Zimbra is available!

Email Client Comparison

	Zimbra Web Client	Zimbra Desktop Client[i]	Outlook	Apple Mail w/iCal	Entourage	IMAP client	POP client
Email & Calendar Combined[ii]	X	X	X		X		
Global Address Book[iii]	X	X	X	L	L	L	L
Mail looks the same anywhere[iv]	X	X	L[v]	L[4]	L[4]	L[4]	
Address Book contacts are the same anywhere[vi]	X	X	X	X	X		
Vacation messages[vii]	X	X					
Shared Mailboxes	X		X		?		
Shared Calendars[viii]	X		X	?	?		
View Free/Busy times of others to schedule meetings	X	X	X				
Ability to store more mail than your quota[ix]			X	X	X	X	X
Mobile Device connection[x]	X	X	?	?	?	?	?
View mail offline[xi]		X	X	X	X	X	X
Requires configuration[xii]		X	X	X	X	X	X
Online Briefcase (Document Storage)[xiii]	X	X					
Zimlets[xiv]	X						
Document editing & sharing (Wiki)[xv]	X	X					
Tasks[xvi]	X		X	X			
View your quota[xvii]	X						

X: Full functionality
L: Limited functionality
?: Currently untested/unconfirmed

[i] Windows XP SP2 and above, Mac OS X (Intel) Tiger 10.4.11 or Leopard 10.5.4 and above, and Linux (x86) 2.6.x and above

[ii] With Zimbra, you won't have to sign into a second application to view your calendar. Your mail and calendar are together for your convenience.

[iii] All HSU addresses are stored in the Global Address Book so you don't have to open a web page to lookup an HSU email address.

[iv] When your mail is stored on the server (online), you can see all of your messages no matter where you are. If you use Zimbra, the interface (buttons, menus, etc.) is the same whether you are in your office or on the go.

[v] These applications will allow you to keep your mail on the server; however you would also have the option to store some of your mail on your computer (if you run out of space in your mail box). Any mail you move to your computer would not be available through the zimbra webmail interface. Additionally, the interface (buttons, menus, etc.) would be different between your email client and the webmail interface.

[vi] Your contacts are stored on the server so they will be the same whether you are in your office or on the go.

[vii] Easily set an auto-reply message to go out when you are out of the office. This runs on the server, so you don't have to leave your email client open while you are out of the office.

[viii] You can now share your mailboxes and calendars with other HSU users. You decide whether someone can read only, read and write, or have no access.

[ix] With Zimbra, you must stay within your mailbox quota (100 mb for students, 500 mb for faculty and staff). If you have difficulty staying within this limit, you may need to use a client that allows you to save messages on your computer. Any mail you move to your computer would not be available through the zimbra webmail interface.

[x] Zimbra has tools to connect with nearly every mobile device.

[xi] If you ever take your laptop somewhere that has no Internet connection and you need to read your email that is already downloaded (cached), you should choose a client that allows you to view your cached messages while offline.

[xii] The Zimbra Web Client gives you instant access to your mail and calendar without any technical configuration. All of the other client options require varying degrees of configuration.

[xiii] Zimbra allows you to save documents to your Briefcase. You can access these files from any computer connected to the Internet. You'll never have to e-mail yourself a file again. Please note that anything stored in your Briefcase counts against your quota.

[xiv] Zimlets are tools built into Zimbra that help you increase productivity. For example, you can easily view your appointments by hovering over a date in an email

[xv] Zimbra allows you to create simple documents and edit them online. You can also collaborate on these documents with other Zimbra users. Please note that anything stored in your Documents counts against your quota.

[xvi] Keep track of your tasks and to do lists right from your email client.

[xvii] Knowing how much of your quota you are using is important to keeping your inbox from filling up. Zimbra displays your quota so you will always know where you are.

Zimbra Details for ITCs

Quotas:

Faculty/Staff - 500MB

Student - 100MB

Dates:

Dates are outlined in the document titled “Email and Calendar changes coming soon!”

Clients:

Client choices are outlined in the document titled “Email and Calendar changes coming soon!” as well as “Email Client Comparison”. These documents will help you and your users make an informed choice.

Educational Campaign:

We will have an educational campaign in September to get users to clean out their mail. We will tell them what they should/can throw away and give them tips on how to do so effectively. We will suggest that they file their attachments on their local computer rather than using e-mail as a storage place for those.

We will have other security/file retention related issues included in this campaign.

Migration:

Any mail that is on the server (primarily that of webmail or IMAP users) will be moved to the new Zimbra server via IMAP sync.

ITS will provide migration training to staff (ITS/ITCs/student workers) prior to the cutover.

ITS will have a handout outlining "basics" to pass out to users during migration.

ITS will have Calendar training courses during the Calendar migration period before the Zimbra roll-out.

We will have training courses on how to use Zimbra during the first X (?) weeks after the cutover.

On Z-Day (October 20, 2008), the names imap.humboldt.edu, pop.humboldt.edu, smtp.humboldt.edu, and webmail.humboldt.edu will be pointed to the Zimbra mail

server. Commercial certificates have been acquired for these names so that email clients will continue to work without any user intervention after the cutover.

This will provide us/ITCs time to migrate users to the Zimbra web or desktop client.

We will provide a team of students and ITS staff to assist ITCs in migrating their users to the extent desired by the ITCs.

With everyone having their mail files nicely under 500 MB, we will provide instructions (for the ITCs) on how to IMAP messages back "up" to the server (Outlook users can use the pst migration tool).

For IMAP users:

* Drag from local folders up to server folders
* Disable Account/Rename Client/Something
* Start using Zimbra

For POP users:

* Disabling the current pop connection
* Creating a new IMAP connection
* Drag from local folders up to server folders
* Disable Account/Rename Client/Something
* Start using Zimbra

We will have the above migration instructions for all of our currently supported clients (Eudora, Outlook, Entourage, Mac Mail, Thunderbird)

HUMBOLDT STATE UNIVERSITY
Response Summary Sheet for
Internal Control Questionnaire/Request for Documents (ICQ/RFD) from Office of the University Auditor

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
	Audit Step Ref. F - Security Policy					
D1	Copy of comprehensive campus information security policies	X			To be coordinated with current rollout of comprehensive CSU system-wide security Policy and Standards (current draft versions are referenced)	CSU_Policy_V01_041808_Released.pdf CSU_Standards_050608_Released.pdf (Moodle ITC documents)
	Audit Step Ref. G - Information Security Organization					
D2	IT and Info Sec Organizational Charts	X	X	X	Need org chart from ITCs showing their roles within their respective organizations	No response yet from Administrative Affairs (Business Svcs., CMS) or CNRS
D3	Information security org charts and job descriptions for employees with security responsibilities	X	X	X	Need from ITCs in organizations where they and/or other staff in the unit have specific information security responsibilities	Some ITC responses are informal only No response from Bus. Svcs. or CNRS
D4	Campus security committees and/or working groups documentation including membership, mission, objectives and meeting minutes from 2007 to current	X	X		ISO will provide for Information Security Steering /Incident Response Committee and for planned Data Custodians security committee; Chair Mark Hendricks will provide for IT Council	M. Hendricks - ITC membership, meeting notes, etc. (some already on Moodle site) JMcB - background docs for InfoSec Executive Committee and Data Custodians Group
D5	Listing of all laptops, servers, or personal computers which were reported as lost or stolen from 2005 to current	X		X	Have sent request to UPD. ITCs may have data from their own areas?	Have sent requests to Tom Dewey and Ed Gordon
D6	Listing of staff affiliations with professional IT/Security organizations (i.e.., SANS, Bugtrack, Campus/local police, FBI, Infraguard, etc)	X	X	X	To be provided by ISO, ITCs and other technical staff with security responsibilities	Educause,ISAC, ITAC, NTA, etc. as well as security-oriented groups
D7	Copy of standard liability, confidentiality clauses and or non-disclosure agreements required of IS/IT procurement service contracts with external vendors (i.e.., IBM maintenance contract, etc)	X			Checking with Business Office, CIO, Risk Manager, ITCs, others; have received copies of two main contract addenda documents from Dave Bugbee	CRL050.pdf - "CSU General Provisions for Service Acquisitions" CRL063.pdf - "CSU General Provisions for Information Technology Acquistions" (Moodle site)
D8	Listing of most recent 20 IS/IT service contracts/agreements where system access is granted or vendor has access to confidential information (electronic or paper). This list should include contracts for CashNet, Document Imaging systems, Secure Document Shredding, Secure PC Recycling/E-waste removal, PeopleSoft consulting services not affiliated with CSU systemwide contract, and any other relevant third party services.		X	X	Update: Specific contracts to be included have been added by OUA. Will need documentation from Business Services, CMS, others.	Need from AA/Business Services/CMS
	Audit Step Ref. H - Asset Management					
D9	Listing of all technology assets (inventory of PCs, laptops, servers, etc) with identification of the respective custodians for each asset		X	X	Will use ITS annual surveys as starting point	In process of being collated
D10	Listing of all designated custodians of records on campus	X			Most functional areas are included on web document, but some need to be added	HSU "Student Records Access Policy," http://www.humboldt.edu/~hsupres/uml/uml03-03.html

HUMBOLDT STATE UNIVERSITY
Response Summary Sheet for
Internal Control Questionnaire/Request for Documents (ICQ/RFD) from Office of the University Auditor

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D11	Campus policy for technology asset disposition, including any data wiping procedures involved	X			Under revision and coordination with Campus Sustainability Coordinator following current CSU system-wide draft Policy and Standards	ISO/ITS will write formal procedures for secure media destruction for approval by IT Council and other relevant groups
D12	Listing of all software site licenses	X	X	X	Received initial list from ITS	ITS_2008_2009_site_license_list.xls
D13	Listing any other software license packages used on campus	X	X	X	Need lists from both ITS and ITCs	
D14	Campus acceptable use policy for computers and systems	X			System-wide AUP under review; Humboldt's AUP document is available on web site	www.humboldt.edu/~its/planning/policy/aup.shtml; pdf version also available
D15	Campus data classification policy	X			CSU System-wide data classification policy is in draft form	CSU_Standards_050608_Released.pdf (Moodle site)
D16	Procedures for identifying and inventorying sensitive data	X	X	X	Critical priority for campus risk management	Part of Payment Card Industry (PCI/DSS) requirements; will add to agenda for meeting between ISO and AA/Business Svcs.
D17	Procedures and relevant employee training for the labeling and handling of sensitive data	X			Expected module of CSU System-wide information security online training course rollout during 2008-09 academic year	ISO will follow up with HR
	Audit Step Ref. I - Human Resources Security					
D18	Policies and procedures for background checking employees with access to sensitive/confidential information	X			Obtain from HR, Academic Personnel	ISO will follow up with HR
D19	Campus confidentiality agreement for any party (employee, contractor, etc) granted systems access	X			Have forms in place for faculty, staff. Need to ascertain use of forms for student employees. General site for faculty, staff and contractor forms is http://www.humboldt.edu/~hsuhr/forms/	http://www.humboldt.edu/~hsuhr/forms/docs/HSU_Confidentiality_Staff.pdf http://www.humboldt.edu/~hsuhr/forms/docs/HSU_Confidentiality_Faculty_8_06_000.pdf Check w/Business Office for Contractor confidentiality agreement forms
D20	Third party contracts standard language for information security responsibilities (may overlap with D8)	X			Cf. item D7 above	CRL050.pdf - "CSU General Provisions for Service Acquisitions" CRL063.pdf - "CSU General Provisions for Information Technology Acquistions" (Moodle site)
D21	Documentation of any specific information security training provided throughout the campus (encryption, fax machine usage, laptop usage, access, passwords, email usage, etc) - May overlap with D17.	X			cf. various ITS Information Security web pages; check with ITCs re any additional security training. Overall training expansion planned as part of CSU System-wide information security online training course rollout during 2008-09 academic year	In process
D22	Policies and procedures for employee non-compliance with campus data policies or committed security breaches	X			Check w/HR, Academic Personnel	ISO will follow up with HR
D23	Procedures for notifying terminated employees and contractors of their ongoing responsibilities for maintaining info security	X			Check w/HR, Academic Personnel	ISO will follow up with HR

HUMBOLDT STATE UNIVERSITY
Response Summary Sheet for
Internal Control Questionnaire/Request for Documents (ICQ/RFD) from Office of the University Auditor

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D24	Copy of campus employee clearance form	X			General site containing HR forms, including clearance forms, is http://www.humboldt.edu/~hsuhr/forms/	Separating employee clearance form: http://www.humboldt.edu/~hsuhr/forms/docs/SepEmpClearance_04_08.pdf; separating *Housing* employee clearance form: http://www.humboldt.edu/~hsuhr/forms/docs/housingclear.pdf
D25	Procedures for removing user IDs from security groups / servers, etc. from systems with sensitive/confidential/protected data upon termination of the user.	X	X	X	ITCs to supply local procedures used by them; also check w/HR, Academic Personnel	ISO will check with Banner; will add to list of items needed from CMS
D26	~~Policies and procedures for the daily operations of the systems & servers (exchange, web, op systems)~~				Item removed by OUA as of 7/16/2008.	N/A
	Audit Step Ref. J - Computer Operations Management					
D27	Procedures for change control within networks and servers	X	X	X	Have some ITS procedures in place; need local procedures from ITCs	ISO will coordinate additional formalization of change control procedures
D28	Procedures for monitoring and managing the use of network resources across the campus	X	X	X	"	ISO will obtain from CITSS; may also need from Auxiliaries
D29	Procedures for running network scans checking for viruses and malicious code (listing of security scanning tools and frequency of use)	X	X	X	"	ISO will obtain from CITSS
D30	~~Documentation of computer operator problem logs with description and disposition~~				Item removed by OUA as of 7/16/2008.	N/A
D31	Current contract with Iron Mountain or other backup transit/storage facility	X	X	X	Need copy of current ITS procedures re remote backups recycling to/from Sonoma State Univ.; need any local backup plans/contracts from ITCs	ISO will obtain from CITSS
D32	Procedures and contractual arrangements for fail-over replication sent off-site to another CSU campus (including web, SQL, email servers)	X			Need to clarify whether HSU has any such off-site business continuity agreements beyond backups to Sonoma State	ISO will obtain from CITSS
D33	Entire campus network diagram/map	X	X	X	Need updated logical/physical network security diagram from TNS; need similar from ITCs who manage network resources, e.g., for Auxiliaries	ISO will obtain from CITSS
D34	Procedures for controlling and securing the campus networks, including the campus wireless service (authentication of users, network service usage restrictions, etc.)	X	X	X	Need from ITCs who manage own network wireless resources, e.g., ResNet, others?	General user requirements, allowed ports, etc. are at http://www.humboldt.edu/~its/techguides/connection/wireless/
D35	~~Policy for restricting and controlling the storage of files on removable media (encryption, etc.)~~				Item removed by OUA as of 7/16/2008.	N/A
D36	Listing of all disposed PCs, laptops and servers	X	X	X	Need from both ITS and from ITCs who manage disposal of local resources	ISO will check with HSU Sustainability Coordinator
D37	Protocol for the disposition of sensitive information and for logging of machines wiped prior to disposition	X	X	X	"	see item D11

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D38	~~Procedures for the secure storing of system documentation (network maps, etc.)~~				Item removed by OUA as of 7/16/2008.	N/A
D39	Procedures for the encryption of application databases and network transmissions	X	X	X	Need from both ITS and from ITCs who manage local networks, resources or applications that utilize encryption	ISO will obain from CITSS; will add to list of items needed from Bus. Svcs. / CMS
D40	~~Policy for acceptable use of instant messaging services for university business~~				Item removed by OUA as of 7/16/2008.	N/A
D41	Procedures for managing online business transactions (especially auxiliaries) or documentation of third party contractors managing online transactions	X	X	X	Need from both ITS and from any ITCs whose units support third party contractors managing online transactions	ISO will add to list of items needed from Bus. Svcs. / CMS. May need additional documentation from Auxiliaries' ITCs
D42	Policies and procedures for ensuring security of campus web systems (SSL, VPN, etc.)	X	X	X	Need from both ITS and from any ITCs whose organizations manage 'in house" web servers or applications	May need to create formal policies through IT Council
D43	Policies and procedures for managing, securing, and reviewing audit logs and security event logs of operating systems, servers and applications (log management and alarm implementation)	X	X	X	Need from both ITS and from any ITCs who manage systems, servers or applications	May need to create formal policies through IT Council
	Audit Step Ref. K - Access Control					
D44	A listing of all applications which contain "protected level-one data" (campus and auxiliaries); and any corresponding risk assessment or conclusions	X	X	X	Essential information needed from ITS and ITCs	No response from Bus. Svcs. / CMS or CNRS
D45	Listing of all user IDs (excluding students) and their assigned roles within each of the critical applications with sensitive data (PS Finance, PS HR, PS Student, CashNet, Medical Records system, etc.)	X	X	X	Need this from ITCs in areas listed or in any other area whose users deal with "protected level-one data"	Need from Bus. Svcs. / CMS and from Student Health Center
D46	Documentation of the workflow form or process required for system access requests	X	X	X	Need this especially from ITCs in every area that deals with "protected level-one data" but also from all ITCs with security management responsibility for systems (authentication and/or authorization responsibility)	Need to create formalized procedures if none exist
D47	Documentation of procedures or forms required for granting privileged access	X	X	X	"	Need to create formalized procedures and/or forms if none exist
D48	Documentation of the periodic review (done by each department or division) of user access roles/permissions for the reconciliation of what access actually exists (per access lists) to what access should exist (per dept inquiry)	X	X	X	"	Need to create formalized procedures if none exist
D49	Screen print of active directory group policy for password management	X	X	X	Need from all ITCs who manage their own Active Directory domain entities	Open request
D50	Listing of any applications/servers which maintain user access rules independent of active directory	X	X	X	Need from all ITCs whose area of responsibility encompasses such applications/servers	Open request
D51	~~Campus policy for unattended screens, clear desk policy~~				Item removed by OUA as of 7/16/2008.	N/A

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D52	Documentation of network segmentation (VLAN)	X	X	X	Need campus-wide VLAN and security zone documentation from TNS; need local VLAN documentation from any ITCs who manage local VLANs within their scope of network management	ITS will obtain from CITSS; also need from ITCs where relevant
D53	Documentation (screen prints) of group policies for each active directory domain	X	X	X	Need from ITS centrally as well as from all ITCs who manage AD domains	Open request
D54	Policies and procedures (and group policy rules) for user ID naming conventions	X	X	X	Need from ITS centrally as well as from all ITCs who manage local ID resources	Open request
D55	~~Policies and procedures (rules and restrictions) for restricting the use of systems tools~~				Item removed by OUA as of 7/16/2008.	
D56	Documentation of group policy rules for network and application sessions (time-out, etc.)	X	X	X	Need from ITS centrally as well as from all ITCs who manage local AD domains or network and system resources	Open request
D57	Procedures for the periodic review of user account deletions (i.e. review of payroll reports distributed to ITS and CMS)	X	X	X	Need from ITS and CMS, as well as from any ITCs having security management over local systems and resources	Need to clarify current procedures and formalize if necessary
D58	Policies for the security of mobile/remote computing (tele-commuting, etc.) and procedures for the approval of such arrangements	X	X		Likely to emerge as part of CSU system-wide policies and standards	Awaiting more specific CSU direction; will check with HR re campus policies
D59	Listing of all independently managed servers that do not participate in the auto-update virus patch software provided by ITS (likely servers that could not be determined/defined from internal port scanning as a result of internal firewalls installed)	X	X	X	Need from ITCs a listing of any servers they manage that do not have procedures or methods to assure that they receive campus-wide anti-virus updates made available by ITS	Open request
	Audit Step Ref. L - Incident Response					
D60	Policies and procedures for security incident response (for networks, systems, etc) resulting from incidents such as system failures and loss of service, malicious code, denial of service, breaches of confidentiality and integrity, misuse of info systems	X	X		ISO will be coordinating HSU procedures with CSU system-wide policy and standards	CSU-wide procedures are on CSU protected wiki site
D61	Procedures for the formal reporting of security weaknesses and incidents in systems or services	X	X		"	CSU-wide procedures are on CSU protected wiki site
D62	Listing of any significant security incidents and/or data breaches from 2005 to 2008	X	X		Have listing of incidents from July 2007 to present; need to research existence of earlier records	2007-2008 list is available from ISO on request
D63	~~Policies and procedures for the collection of electronic evidence and forensics~~	X	X		Item removed by OUA as of 7/16/2008.	N/A
	Audit Step Ref. M - Compliance					

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D64	Procedures for intellectual property rights compliance with reference to software license agreements (legal review, copyright law, asset registry, user limitations, monitoring of software installed, general use)	X	X	X	ISO will be coordinating HSU procedures with CSU system-wide policy and standards	cf. Appropriate Use Policty at www.humboldt.edu/~its/planning/policy/aup.shtml President's letter re music sharing, 2005, at http://www.humboldt.edu/~hsupres/email/020105.html HSU Copying Policy, 1990, at http://www.humboldt.edu/~cdc/policy/copyright.html
D65	Procedures or action plan for compliance with EO 1027 for record retention	X	X	X	Current campus initiative	ISO will add to list of items needed from Bus. Svcs. / CMS. May need additional documentation from Auxiliaries' ITCs
D66	Procedures for compliance with HIPAA, FERPA, GLBA, SB 1386, SB 25, PCI DSS	X	X	X	Some compliance documentation is current, in other cases needs to be formalized or updated	cf. HSU's formal Information Security Program (2003) document at http://www.humboldt.edu/~its/techguides/security/isp6803.pdf
D67	Procedures for the campus response to information requests under the CA Public Records Act (validation of subpoenas prior to divulging sensitive information)	X	X	X	Need to check with Public Affairs and/or UPD for additional information	Basic procedures on HSU website at http://www.humboldt.edu/~marcom/mediaRelations.php?section=publicRecords
D68	Listing of all locations on campus which accept credit cards (all satellites, auxiliary orgs, etc) with identification of any third-party services utilized	X	X	X	Need from Business Svcs. and possibly Auxiliaries	ISO will add to list of items needed from Bus. Svcs. / CMS. May need additional documentation from Auxiliaries' ITCs
D69	Procedures for use by the Information Security Officer to ensure PCI DSS self-assessment and any documentation of reviews done for PCI DSS compliance, including documentation of any quarterly network scans	X	X	X	Under development by ISO; need to gather additional documentation regarding individual Offices' or Auxiliaries' PCI DSS audit reviews, etc.	Part of Payment Card Industry (PCI/DSS) compliance; will add to agenda for meeting between ISO and AA/Business Svcs.
D70	Procedures for, and documentation of any compliance reviews or self-assessments conducted relating to compliance with security policies, standards, and any other security requirements (governmental, industry-driven, etc.) - May be performed by the campus ISO or by departmental management for each area.	X	X	X	Formal periodic risk assessment at campus (ISO) level is currently included as part of CSU system-wide draft Information Security Standards; will be coordinated with that document	Formal risk assessment planning expected to commence during 2008-09 academic year
D71	Documentation of any ongoing analysis of health services offered to determine the campus HIPAA status	X	X	X	Need to research relevant factors for determining or reviewing HIPAA status	ISO will follow up with Director of Student Health Center
D72	Documentation of any departmental reviews of system compliance with governmental info sec requirements and identification of any non-compliant issues noted/corrected	X	X	X	ISO will need to collect and monitor results of any recent information security-related audit reviews undergone by individual departments or auxiliaries	Open request for recent system reviews, audits or audit findings
	Audit Step Ref. N - Web Development					
D73	Procedures for management approval of web development projects	X	X	X	Will need to obtain from all areas engaged in web development projects	What does the campus consider a web development project? What is the process for approval?

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D74	An up-to-date schedule of current web development projects, timelines, and deliverables	X	X	X	"	Need to determine source of this information - Marketing and Communication? CMS? Others?
D75	Procedures for the testing and acceptance of web projects (validation checks, vulnerabilities, etc.)	X	X	X	"	Especially any non-centralized CMS development work by Bus. Svcs.
D76	Documentation for when web encryption occurs, at what level and in what state (at rest, in-transit or in databases).	X	X	X	"	"
D77	Procedures for the protection of source/production program code (and tracking of changes made)	X	X	X	"	"
D78	Procedures for the handling, control and protection of system test data	X	X	X	"	"
D79	Procedures for restricting access to program source code	X	X	X	"	"
D80	Documentation of the formal procedures of system acceptance criteria and approval required before going live with changes or upgrades	X	X	X	Some procedures exist relating to approval of systems before allowing them public access through HSU firewall	Need web developers' system acceptance and go-live procedures
D81	Procedures for the management of new technical vulnerabilities	X	X	X	Base procedure should include periodic application scanning with updated tools	Need quarterly scanning of web sites as part of PCI/DSS compliance; will add to agenda between ISO and Bus. Svcs. re PCI Compliance
D82	Examples of reports run to test for technical vulnerabilities	X	X	X	Will need to develop as part of a formal vulnerability testing process for both ITS- and ITC-managed systems	Also related to PCI compliance
	Audit Step Ref. O - Email Systems					
D83	Policies and procedures for email usage, administration, ownership and maintenance		X	X	need documentation from ITS and any ITCs running email servers	Open request
D84	Listing of all known email systems utilized by the campus	X	X	X	"	ISO will obtain from CITSS
D85	Documentation of all security measures (corrective, detective and preventative) regarding malicious software (viruses, Trojan horses, spam filtering) at the sever and desktop level	X	X	X	"	-Centralized Symantec A/V deployment (pushed to desktops, available to servers) -Reports from REN-ISAC re possible bot traffic -Examination of anomalous network traffic -Other measures?
D86	Documentation of security provisions to minimize email spoofing and prevent message relaying	X	X	X	"	cf. secure email client setup procedures at http://www.humboldt.edu/~its/techguides/email/setup.shtml
D87	Policies for email retention and backup	X	X	X	"	ISO will obtain from CITSS
D88	Procedures for reporting malicious events and other misuse of email	X		X	"	ISO will obtain from CITSS
D89	Procedures for the management and security of email servers	X	X	X	"	ISO will obtain from CITSS

HUMBOLDT STATE UNIVERSITY
Response Summary Sheet for
Internal Control Questionnaire/Request for Documents (ICQ/RFD) from Office of the University Auditor

Req.		Need documentation from:				
No.		ISO	ITS	ITCs	Notes	Tasks/Deliverables
D90	Procedures for controlling information leakage via email and other communications (i.e., restrictions on transmitted file types and/or size)	X			Need to clarify whether such procedures intended to address "information leakage" currently exist on campus	Open request

Ref #	Document	CSU Contact Rep	Date Requested	Dated Received	Comments/ Clarifications
	Internet Footprint Analysis				
1	External IP Ranges/Blocks for **the campus (usually a Class B).**				
2	Network diagrams and representative DMZ architecture (e.g. 3 tiered with connections to internal databases or completely flat and isolated).				
	Operating System Platform - Servers				
3	Network server diagrams for in-scope servers.				
4	IP Addresses and host names of production critical servers (Windows and/or UNIX). 5 - 10 servers, **we use this list to select servers to be tested.**				
5	Security configuration baseline and hardening standards for servers.				
6	Change management policies and/or procedures for configuring servers.				
	Website Vulnerability Assessment				
7	IP address and host name of web application servers or web portals housing critical applications (**possibly including auxiliary web applications)**. 3 - 5 servers, we will **select a target** from the identified list. **Servers on this list may include web apps that perform authentication, financial transaction processing, or connect to multiple backend systems**				
	Border Firewall Settings				
8	IP address or host names Core Firewalls facing the internet (per location).				
9	Sample of logs/alerts from core firewall device to confirm logging is enabled.				
10	Policies/procedures to manage the ongoing configuration for changes to core firewall devices.				
11	Firewall policy, configuration sets, filters and access control lists.				

	Router / Switch devices				
12	IP address or host names of Core Routers and Switches facing the internet **or restricting network traffic from critical systems / subnets.**				
13	Document, policies and hardening standards for routers/switches.				
14	Sample of logs/alerts from core routers and switches to confirm logging is enabled.				
15	Procedures in place to manage the ongoing configuration for changes to core firewall devices.				
16	Provide Access Control Lists (ACLs) and/or configuration files for in-scope devices.				
	General				
17	Campus security standards, policies and/or procedures.				
18	A list of Domains or IP-addresses that are considered "do not touch"				