

IT Council Agenda

Next Meeting: Tuesday, February 10th, 2009

Location: NHE 106

Time: 2:00 P.M.

I. Approval of the Minutes

<http://www.humboldt.edu/~its/planning/committees>

II. Working Group Report Items

1. Desktop Support Wk Group (DSWAG): Darnall
2. Network Advisory Group (NAG): Meyer

1 Discussion Items/Action Items

1. File Encryption: Darnall
2. Password Aging : Rizzarda
3. NAG Charter: Meyer
4. HOP Computer Orientation pilot project - Summer 2009: Walker

IV. New Business

1. ITAC Update: Kircher
2. Firewall Closed Border Document: Hendricks
3. Security Incident Procedures: Hendricks

V. Announcements

1. Information Security Documents Work Sessions - February: Hendricks
2. Auto PoE has been successfully disabled campus wide: Ventuleth

VI. Adjournment

Information Technology Council
Humboldt State University

Meeting Notes for: February 10, 2009 from 2:00 to 4:00 P.M., NHE 116

Members Present: Mark Hendricks (Chair), Dave Pearson (CPS), Steve Darnall (CAHSS – proxy for Megan McKenzie), Dale Sanford (OEM), Toby Walker (SA), David Peters (BIS – proxy for Dave Rowe), Cassandra Tex (SDRC), Jeremy Shellhase (Library), Jeanne Wielgus (DITSS), Rick Garcia (TNS), Dave Marshall (CNRS), Drew Myer (Housing), Kim Vincent-Layton (CELT)

Others Present: Anna Kircher (CIO), Chris Hansen (CAHSS), Bethany Rizzardi (DITSS), Greg Osburn (OEM), Scott Ventuleth (TNS), Lorrie Marsh (TNS), Ed Albert (UPD), Molly Simpson (Recorder)

1. Approval of the Minutes:

January 13, 2009 minutes were approved as distributed (Marshall/).

2. Report Items:

NAG: Meyer reported that the group had been meeting. The group charter was reviewed and changed. The main difference in the revised charter is that the Network Advisory Group (NAG) will now represent the campus technology community at initiative meetings. Discussion ensued regarding future topics to be addressed by NAG. This group meets on the third Thursday of each month at 2:00 P.M. in JJC.

DSWAG: Darnall reported that the software update server is now running. Darnall told the Council that the DSWAG discussed issues with using SKYPE. He noted that if incorrectly installed, SKYPE can become a “super node” that may result in network saturation. The Council was asked to provide a campus SKYPE Practice. Kircher asked that the practice include ways to mitigate problems. Ventuleth stated that SKYPE should not be allowed on wireless. The topic was forwarded to the NAG for discussion. Darnall also noted that the Symantec Anti-virus will expire in July/August. A motion was passed to have DSWAG review campus anti-virus options.

3. Discussion Items/ Action Items:

Wireless Equipment and Switches: Garcia discussed the upcoming ITRP2 wireless project. The issue of prioritization was raised by Garcia. The topic was referred to NAG

Encryption: The Council discussed the need for an encryption strategy for the campus. A group was formed to review encryption issues and address information security related encryption topics.

Password Expiration for Staff: Rizzardi reviewed password expiration processes and documentation. Current focus is to educate the campus about the password expiration process and notification. Rizzardi noted that hot links would not be sent in email notifications and the email will have an ITS template to help distinguish legitimate requests from phishing. Forgotten password recovery/reset tools are close to being completed, and information regarding the tools will be distributed soon. DSWAG was asked to look into the creation of a login splash screen.

NAG Charter: see NAG report.

HOP Computer Orientation Pilot Project: Walker told the Council that HOP is in the process of putting together a pilot project for students. Four half-hour sessions will be developed to address topics like lab survival skills (wireless, WebReg, equipment on campus) and Ethics (copyright & phishing scams). Walker noted that suggestions would be appreciated and asked that they be forwarded to him. HOP will be meeting again in March.

4. New Business:

ITAC Update: Kircher reviewed a list of common findings from Information Security Audits (re-capped by Greg Dove 2/2/08 ITAC telephone conference) She noted that D67 (procedures for campus response to requests under the California Public Records Act) should be discussed at a future IT Council meeting. Kircher told the Council that the Incident Response document will be completed and brought to a Council meeting soon. Kircher reminded Council members about the work sessions for audit related documents and encouraged participation.

Firewall Closed Border Document: Hendricks reviewed the draft process for HSU campus border firewall closure noting that the border will be closed on October 1, 2009. On-line forms for requesting border exceptions will be available by April 1st. Hendricks noted that the plan outlined in the closed border document states that after the border has been closed, temporary exceptions will be granted if requested. Campus IT staff will have until August 1st, 2009 to register all Internet facing servers, and their exceptions. TNS will have two months to monitor and resolve any issues prior to the border closure. Hendricks

submitted the document for review. Discussion ensued regarding the document. Document will be submitted for approval at the next Council meeting.

Security Incident Procedures: Already covered by Kircher

5. Announcements:

6. Adjournment: 2:35 P.M. (Marshall/Pearson)

January 29, 2009 DSWAG Meeting Summary

1. WSUS

- The WSUS server is working.
- Mark will look into sharing part of the console. If that is not practical/wise, he would be willing to report out of date systems.

2. Skype

- CAHSS has had requests for Skype on a classroom computer and in faculty offices; some Faculty members have been using Skype on campus with their own notebooks. It was asked of the group whether they allow Skype on their systems and if they have any policies or concerns with its use. The biggest concern is security; another is non HSU network traffic being routed through an HSU system; thus taking up bandwidth. There is now available a version of Skype that prevents a station from becoming a “super nodes.”
- Mark Hendricks will look into the security issues and bring up Skype for discussion at the next ITC meeting.

3. Symantec

- Some Symantec licenses expire on July 29, the rest on August 15. It was agreed that DSWAG request a charge from the IT Council to develop a list of questions to be considered when assessing potential anti-virus software solutions.

4. Presentations and requests for assistance

- There was not enough time for the presentations and requests for assistance from Sergey Brin, Larry Page, and Larry Ellison.
- They handled their disappointment well (getting Darnall's autograph helped) and asked if they could return when Bill Gates presents. We agreed that they could return - with the clarification that we might not have time for their presentations or questions on that date either. They were ecstatic and oh so grateful for our consideration in this matter.

Network Advisory Group (NAG)
Working Group
Informational Technology Council

Draft Charter

Scope Of the Group

The Network Advisory Group is formed to:

1. Identify issues concerning campus network operational practices and advise the Information Technology Council and Information Technology Services (ITS) on potential improvements.
2. Advise ITS and the IT Council on system wide initiatives on campus.
3. Respond to specific requests for information or guidance from Information Technology Council and Information Technology Services (ITS).
4. Represent Technology community at initiatives meetings.

Term

On-going

Membership

Meetings are open to all interested members of the technology community

Meeting Times

Third Thursday of the Month

Location

JGC Mad River Room

Draft process for HSU campus border firewall closure

Background:

In 2006 Humboldt State University was provided two enterprise class firewall devices by the Chancellor's Office as a part of ITRP2 (Infrastructure Terminal Resources Project). Since the border firewall installation, the firewalls have provided limited security and risk mitigation because they are configured to "allow by default". Translated into English this means that HSU is directly connected to the Internet with little or no protection. Any hacker in the world can easily identify common vulnerabilities and attack computers directly. With a "Default Allow" configuration, only traffic that is specifically "denied" is blocked. This is known as an "open border." Various international standards for information security identify this as an unacceptable risk, ITRP standards have identified this as an unacceptable risk, and continuing this practice will result in an IT security audit finding. Instead, computer security experts (*and Section 9 of THE CALIFORNIA STATE UNIVERSITY SYSTEM-WIDE INFORMATION SECURITY STANDARDS document*) recommend that firewalls be configured to "deny incoming traffic by default" unless specific exceptions are added.

Why hasn't HSU closed the "border" sooner? Because changing the default policy to "Default Deny" is not a trivial undertaking. All too often, network enabled applications use one or more "ports" that are not well documented, requiring a lengthy and detailed documentation and registration process.

Representatives from the campus IT community have discussed this topic in detail and have made the following recommendations:

Network Advisory Group (NAG) Closed Border Process/Time line 2/2/2009

Closing the border firewall is of the utmost importance to the security of campus computers and the data that they contain. Every effort will be made during this process to monitor traffic patterns prior to the cut-over to minimize negative impact to business processes and instruction. During the cut-over period, staff will be available to rapidly respond to and resolve network communications issues should they arise. Efforts will be made to target potential problems through a combination of education, alternate technologies, and temporary exceptions.

1. Beginning no later than April 1st, 2009, on-line forms for Internet Facing Servers and Firewall Exceptions will be available. Campus IT personnel will have until August 1st, 2009 to register all Internet facing servers, and their exceptions.
2. When servers are registered they will be added to a firewall rule that will simply log all inbound traffic that is not covered by the requested exceptions. This log rule will be used to determine if valid port exceptions have been overlooked.
3. An exception for remote desktop will be created by request. This exception will expire during the Winter break. Users of this functionality should be trained to use either network shares for access to data or the VPN solution if access to applications is absolutely necessary. After server registration, and before border closure, TNS/Security will notify users of inbound remote desktop to provide migration assistance.
4. TNS will have 2 months to monitor and resolve any issues prior to border closure. During this 2 month window, firewall exceptions will be performed on a first come first serve basis as time permits.
5. Status of the Closed Border Process will be reviewed with IT Council during its regular

6. A “go/no-go” decision will be made by the CIO 24 hours prior to cut over.
7. Border firewall configuration changed to “default deny” October 1, 2009.
8. A “go/no-go” decision will be made by the CIO within 24 hours after to cut over. If the CIO determines that there is sufficient cause to abandon the upgrade, configuration settings will be returned to their previous state.
9. For a three week period after the cut-over date, temporary exceptions for specific ports will be granted unless it is deemed to cause excessive and unnecessary risk. Temporary exceptions will be immediately granted through the normal firewall change request process, pending a security scan for detectable vulnerabilities based on the most current SANS top 20 security risks.
10. Any temporary exceptions not resolved by January 2, 2010 will be removed.

Misc:

Procurement of a VPN appliance is vital.

Departments should be encouraged to add any server containing Level 1 Confidential data to a deny rule as soon as possible.

Departments should be encouraged to add any subnets to a deny rule if coordination is possible.

Regular firewall reports should be utilized to locate systems that have been overlooked.

HSU Password Expiration (Web Page)

If you receive an email informing you that your HSU Password is scheduled to expire, you **MUST** go to the WebReg and change your password **BEFORE** the expiration date. Visit www.humboldt.edu/change or go to the Humboldt web page (www.humboldt.edu), select Quick Links > WebReg. Once you have logged in, select Account Tools, then Change Password.

Your HSU Password is used to access email, Moodle, PeopleSoft, lab and office computers, and many other systems.

Password Expiration

HSU Passwords will expire at regular intervals, as outlined below:

If you have access to...	Your password will change every...
PeopleSoft Finance	90 days
PeopleSoft HR	120 days

* If you have an access to more than one of the systems above, your password will expire in the shortest number of days. For example, someone with access to PeopleSoft Finance AND HR would have their password expire every 90 days.

Why do I have to change my password?

The requirement to change your HSU password regularly is part of a larger effort at HSU to make campus computing systems more secure. For more information about how computer security issues may affect you and your use of HSU systems, visit www.humboldt.edu/security.

How will I know when my password is about to expire?

Periodic email notifications will be sent well in advance of the HSU Password expiration giving you plenty of notice to change your password. You will see notices at 14, 7, 3, 2, and 1 day(s) before it expires.

What happens if I don't change my password?

If a new password is not set by the expiration date, you will not be able to login to your HSU accounts. You will need to use the "[Forgotten Password Tool](#)" before you can login to any HSU system. This tool is located at www.humboldt.edu/reset and will require that you answer security questions to verify your identity. You should take a moment to provide answers to these security questions now. In [WebReg](#), select Account Tools > Identity Verification questions.

Where do I get help?

If you need assistance or have any questions, contact the Help Desk at 707-826-HELP (4357) or come see us in Lib 120B.

Sample Email

Subject: Your HSU Password Will Expire On ^EXPIRATION_DATE^

FirstName LastName,

The password for your HSU account, XXX7001, will expire at midnight on ^EXPIRATION_DATE^.

You will need to log into WebReg to change your password before this date. If a new password is not set by the expiration date, you will not be able to login to your HSU accounts.

To change your password, go to www.humboldt.edu/change. Login to change your password.

To understand why your password is expiring, please visit www.humboldt.edu/~its/whymypasswordexpiresxxxxx <insert real link>

If your password expires before you get a chance to change it, you can reset your password by visiting www.humboldt.edu/reset. This tool will require that you answer security questions to verify your identity.

If you have questions about the authenticity of this notice, please contact the Help Desk.

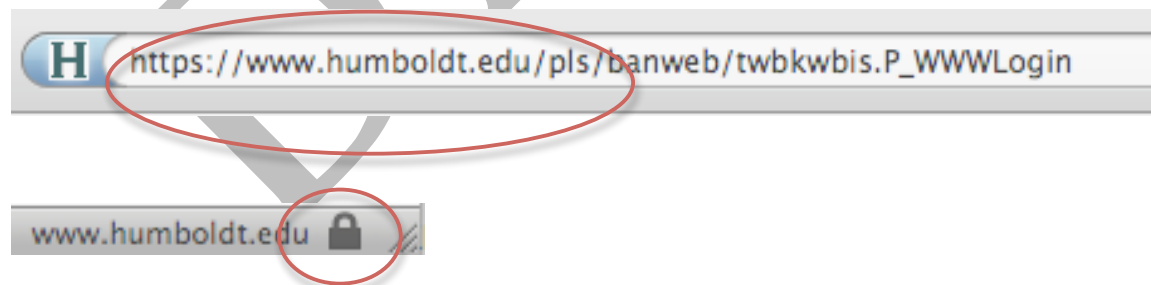
Help Desk

Phone: 707.826.HELP(4357)

Office: Library 120B

E-mail: help@humboldt.edu

Note: To safeguard your private information, you should always verify that web sites asking for personal information are legitimate. In this case, it is important to verify that any web page you visit has a REAL Humboldt web address. A "real" Humboldt address will contain "humboldt.edu" after the first double slashes and before the first single slash. You should also look for a picture of a lock in the corner of your browser.



Appendix

*VERSION 1.0 DRAFT 12
THE CALIFORNIA STATE UNIVERSITY SYSTEM-WIDE INFORMATION
SECURITY STANDARDS OCTOBER 27, 2008*

Section 9.4 Boundary Protection and Isolation

Campus networks must be protected at all ingress and egress points by a device or devices which permit only authorized inbound and outbound traffic; all other traffic must be blocked. The campus must appropriately separate network access to public information system resources from those which store protected Level 1 and Level 2 information. Campuses must establish zoning or separation within its internal networks based on established trust relationships, authorized services, and data classification in order to ensure that protected information is not made available to unauthorized persons. All unnecessary services (e.g., Web server, SNMP) on any campus border device must be disabled. All management connections across a network to campus border devices must be encrypted and authenticated. Direct management connections (i.e., console connections) do not require encryption.

Each campus must have:

- A formal, documented process for approving and testing configuration changes to its network and network control devices.
- Formal, documented network configurations that define all open ports and services.
- Documented justification for any allowed service or protocol.

Protocols known to carry substantial risk of exploit (e.g. telnet, FTP) may be allowed only after risk analysis and justification. Border device configurations and rule sets must be reviewed and revised, as necessary, at least annually.

Firewalls are the main preventive measures that are deployed on most networks. In order for a firewall to properly prevent traffic, it must be designed correctly with all connections going through the it. It must also have rule set that follows the principle of least privilege. It is best practice to configure the firewall to be default deny or only allow the traffic it needs and deny all other traffic. © 2000-2009 The SANS Institute "Firewall Technology and Architecture" <http://www.giac.org/resources/whitepaper/network/12.php>

Links:

THE CALIFORNIA STATE UNIVERSITY SYSTEM-WIDE INFORMATION SECURITY STANDARDS

http://www.humboldt.edu/~its/techguides/security/Systemwide%20Info%20Security%20Standards_v1%20Draft.pdf

ITC 002 Internet Facing Server Procedure

ITC 003 Firewall Change Management Procedure