

Information Technology Council
Humboldt State University

Meeting Notes for: January 13, 2008 from 2:00 to 4:00 P.M., NHE 116

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

Others Present: Anna Kircher (CIO), Josh Callahan (CITSS), Steve Darnall (CAHSS), Mike Bradley (DITSS), Bethany Rizzardi (DITSS), Joan Van Duzer (CELT), Molly Simpson (Recorder)

1. Approval of the Minutes:

December 9, 2008 minutes were approved as distributed (McKenzie/Ventuleth).

2. Report Items:

NAG: Campus Manager Update. Ventuleth distributed an updated Campus Manager configuration document. This document updates the ITC Procedure 008 with a current list of Campus Manager settings as approved by NAG. An additional configuration setting to address access by Linux systems will be evaluated by NAG.

Hendricks announced the Meyer had been elected Chair of the Network Advisory Group (NAG). Meyers announced that NAG would be meeting the 3rd Thursday of each month from 2:00 P.M. to 3:00 P.M. in JJC Mad River Room (2nd floor) The group charter was reviewed at the last meeting and Meyer noted that he would bring the charter to the next IT Council meeting. Future topics for the group include: recommendations on firewall and Active Directory. The group plans to review current Active Directory domains. Meyers told the Council that he would be the liaison for ITRP2 communications to the IT Community. He will report on timelines, outages, etc.

3. Discussion Items/ Action Items:

Information Security Office Changes: Kircher announced that McBrearty had retired from the University effective December 31st. She reviewed the strategy to

maintain the current Security Program noting that governance groups would remain the same:

- IT Council
- Data Stewards Group
- Security Incident Response Group (CSIRT)

For now ISO duties will be distributed to:

- Kircher - Information Security Officer
- Callahan - Technology Security Officer
- Hendricks – Security Analyst
- Garcia – Network Analyst

Any security issues should be sent to security@humboldt.edu. AD issues should continue to be directed to sysadmin@humboldt.edu

ITS plans to move all security documentation on to the Moodle site for better access by campus staff and help the campus consolidate documentation for the upcoming security audit. Kircher noted that she would send the security procedures to ITCs.

Password Expiration for Staff: Password expiration for staff with PS HR and PS Finance access is being enforced. Passwords for PS Finance staff will expire every 90 days; HR staff access will expire every 120 days. Kircher told the group that a training program was being developed to notify campus about legitimate requests for changing passwords.

CATS Conference: Four proposals were received for attendance at this year's CATS conference. Vincent-Layton, Van Duzer, Smart, Hooker (late). Kircher reminded the Council that there are only two sponsored spots this year. She will forward all proposals to the Council to review. A decision needs to be made quickly.

4. **Announcements/New Business:** none
5. **Adjournment:** 2:35 P.M. (Marshall/Pearson)

**HSU-IT-Procedure:
Campus Manager Wireless Configuration
Status: Proposed
Classification: Required
Procedure Number:**

1.0 Purpose

The purpose of this procedure is to establish configuration settings for computers using the HSU Wireless network through the Bradford Campus Manager application.

2.0 Scope

This procedure establishes what Operating Systems, minimum patch levels, and antivirus will be allowed access to the HSU wireless network through the Bradford Campus Manager application.

2.1 Intended audience

Wireless configurations will affect all campus users using the wireless network.

3.0 Procedure

3.1 Configuration Settings

3.1.1 Operating Systems Allowed

The following Operating Systems will be allowed:

- | | | |
|--|--|---|
| <p>Windows:</p> <ul style="list-style-type: none"> ○ 2000 ○ 2003 Server ○ 2008 ○ XP ○ Vista | <p>OS X:</p> <ul style="list-style-type: none"> ○ 10.2 (Jaguar) ○ 10.3 (Panther) ○ 10.4 (Tiger) ○ 10.5 (Leopard) | <p>Linux:</p> <ul style="list-style-type: none"> ○ All <p>Handheld OS:</p> <ul style="list-style-type: none"> ○ All |
|--|--|---|

3.1.2 Service Pack/Patch Level Requirements

This establishes the initial configuration and accommodation for future release of Service Packs or Patch Levels:

Operating System (Windows)	Service Pack Required	Time frame for enforcement next Service Pack
2000	4	3 months from release date
2003 Server	2	3 months from release date
XP	3	3 months from release date
Vista	1	3 months from release date
2008	N/A	3 months from release date

Operating System (OS X Reference Release)	OS Update Version Required	Enforcement of next Update Level
10.2 (Jaguar)	10.2.6	OS must be within 3 versions of current released update
10.3 (Panther)	10.3.6	OS must be within 3 versions of current released update
10.4 (Tiger)	10.4.8	OS must be within 3 versions of current released update
10.5 (Leopard)	10.5.3	OS must be within 3 versions of current released update

3.1.3 Anti-Virus Requirements

OS X will not be required to have Anti-Virus Software. All Windows Operating Systems will be required to have one of the following anti-virus software packages:

- | | |
|--|--|
| <ul style="list-style-type: none"> • AVG-8.0 • Authentium-Command-AV • Avast • Avira-AntiVir | <ul style="list-style-type: none"> • BullGuard • CA-Anti-Virus • ClamWin-AntiVirus • DrWeb |
|--|--|

- EZ-Trust
- Eset-NOD32
- F-Prot
- F-Secure
- GDATA-AntiVirusKit
- Grisoft-AVG
- Kaspersky
- Kaspersky-Anti-Virus-2009
- Kaspersky-Internet-Security
- McAfee-EPO
- McAfee-Enterprise
- McAfee-Home
- McAfee-VirusScan-Enterprise-8.7i
- MicroWorld-eScan
- Microsoft-Forefront
- Microsoft-Windows-OneCare
- Norman
- Norton
- Norton-360
- Norton-Anti-Virus-2009
- Norton-Internet-Security-2009
- PCTools-AntiVirus
- Panda Rising-Antivirus
- Softwin-BitDefender
- Sophos
- Sunbelt-Vipre
- Sunbelt-Vipre-Enterprise-Agent
- Symantec-Corporate
- Trend-Micro
- Trend-Micro-AntiVirus-2007
- Trend-Micro-AntiVirus-2008
- Trend-Micro-Internet-Security
- Trend-Micro-Internet-Security-2008
- Trend-Micro-OfficeScan
- Trend-Micro-SMB
- Webroot-AntiVirus-Corporate
- Webroot-SpySweeper
- ZoneAlarm-Internet-Security
- eTrust

3.1.3.1 Anti-Virus Definitions

Anti-Virus Definition must be current within 7 days.

3.1.4 Anti-Spyware Requirements

Anti-Spyware software will not be required.

3.1.5 Specific Windows Requirements

The following settings must be configured on the Windows computer to connect to the wireless network:

Operating System	Force DHCP	Disable Bridging	Automatic Updates	Enable Firewall	Require Critical Updates	Require Security Updates	Prohibit Home Edition
2000	Yes	N/A	No	N/A	N/A	N/A	N/A
2003 Server	Yes	Yes	No	Yes	N/A	N/A	N/A
XP	Yes	Yes	No	Yes	Yes	Yes	No
Vista	N/A	N/A	No	N/A	Yes	Yes	N/A
2008	Yes	Yes	No	Yes	Yes	Yes	N/A

3.1.6 NAT detection

If Network Address Translation is detected, the host will be blocked from connecting to the wireless network.

3.1.7 Persistent Agent

The Persistent Agent is not required to connect to the wireless network.

4.0 Compliance

Compliance is established and monitored through the Campus Manager application. Configuration settings, such as Operating System Levels, Anti-Virus software definitions, and new Operating systems, will be updated at regular intervals.

5.0 Enforcement

These rules will go into effect on 01-10-2009.

Systems that do not meet these established configuration settings will not be allowed on the network.

Hosts must re-register once a semester. The system will require users to re-register after returning from a break.

6.0 Definitions

Term **Definition**

7.0 Revision History

Action	By	Date
Created	Bethany Gilden	10/17/2007
Draft Procedure	NAG	10/17/2007
RFC Draft Procedure Posted for IT Council	NAG	11/13/2007
Recommended Procedure Approved by IT Council	ITC	Date ?
Procedure Approval Posted	ITC ?	Date ? ?
Reviewed	NAG	01/09/09
Obsoleted		date

<u>Chancellor's Office</u>	
	ITRP2 - Wireless
	ITRP2 - Equipment Refresh
	NSM Upgrade
	ITRP2 - IDP
	ITRP2 - Data Center Firewalls
	StatSeeker Upgrade
	Security Audit
	CMS VPN Tunnel
	TIS Wiring
<u>Campus</u>	
	Facilities Management - Unviersity Annex
	Facilities Management - Insustrial Electric Building
	Facilities Management - Schatz Building
	Facilities Management - KA Building (on hold)
	Facilities Management - Forbes Complex (on hold)
	Library Learning Commons
<u>Departmental</u>	
	University Center - Fiber Pull
	Housing - Dorms
	UPD - PARC building move
	Housing - place network outside firewall
	Campus Apartments connectivity
	Library Café
<u>ITS</u>	
	Firewall - closed border
	Video VLAN
	Data Center
	Web base firewall request form
	Cost Revoery
<u>TNS</u>	
	Campus Manager Upgrade
	Conferencing Service
	Environmental Sensors
	Security Cameras
	Firewall IOS upgrade
	TACACS server
	X-connect verification
	Departmental hosts - software upgrades
	Courtesy phone cutovers to new cable plant
	Telcom Room Cleanup
	Ericsson MD110 upgrade
	Voicemail system replacement
	Coin Operated Trunks
	Payphone Installs/removal
	DBC 203 migration
	Security Scans

HSU Information Security Program Structure

