



Truckee Meadows Community College

Information Technology Operations

Monthly Status Reports

August 31, 2009

Network/Desktop Updates

- IT Operations assumed the role of providing Student Support for password resets
- ITO Academic Computing has completed security cabling for 200 computer stations in the Sierra Building for a total of 412 stations.
- Installed 31 removable rack and caddy systems in SIER-111.
- Reviewed RAM status on all academic workstations and upgraded 12 stations that were 512MB up to 1GB.
- Added a new library catalog access station in Elizabeth Sturm Library
- Upgrade RAM for 31 stations in SIER-111 from 1GB to 4GB.
- Installed new Dell 2330DN printer in RDMT-115 for the Student Government Association

Reiteration

- ITO Administrative Computing has finished the installation of Wake-on LAN as well as Zen 10 on all administrative Windows-based computers.
- ITO Administrative Computing has begun the imaging and delivery of 135 life cycle replacement computers.
- ITO Administrative Computing has implemented a new nightly automatic PC shutdown program.
- ITO Software and Account Management Team have released Service Pack 2 for Office 2007 to all pc's that are using Office 2007.
- ITO Academic Computing has received software request and began creation of the new academic image.
- ITO Administrative Computing will be implementing a new nightly automatic PC shutdown program in the latter part of June.
- ITO Administrative Computing has inventoried and compiled a list of personal computers that are 5 years old and slotted for replacement.
- ITO has added the Nell J. Redfield Foundation Performing Arts Center (RPAC) to the TMCC network and user log in to the domain like all other users do. This will allow for remote sessions to alleviate immediate problems, keep computers up-to-date with critical updates, etc....
- As a result of the NSHE-wide security audit, use of the college's Virtual Private Network (VPN) will be the primary method used by TMCC faculty and staff access to TMCC networked resources and applications. Instructions for setting up VPN access can be found at <http://www.tmcc.edu/ito/helpdesk/faq/>. In addition, results of the NSHE IT Security audit have required TMCC and IT Operations to do the following:
 - Student workstations in academic computer labs do not have access to the administrative network although teacher workstations will continue to have this access. **Impact: Access to the TMCC administrative network/applications from a student workstation will occur through the virtual private network (VPN). This also the procedure to access printers from a student workstation.**
 - (1) Go to <http://sag2.tmcc.edu> using Internet Explorer
 - (2) Log in with your credentials
 - (3) Click on the ActiveX Control warning message that will drop down
 - (4) Click the Citrix Helper package and install
 - (5) Run the Secure Access Client and accept the license agreement
 - (6) Log in again. In the near future, we will have the Citrix Secure Access Client installed on academic computers.
 - All academic computer labs must be managed by IT Operations. **Impact: ITO staff are working with affected academic departments to make the transition over the Spring semester.**
 - Critical security updates must be installed to computers within a week of their release in order to ensure workstations have current security patches. **Impact: Since all systems connected via a hard wire network interface have**

critical updates automatically download, most of the college is covered. However, it is extremely important for laptop users to work with the Help Desk to ensure that every 60 days, their systems are brought it to ensure the latest updates have been successfully installed.

- Authorized computers and network devices must have a permanent network address (IP) assigned for connecting to the TMCC network. **Impact: Computers that are moved from one location to another will no longer automatically receive a network connection. Similar to how we handle moves of telephones, connectivity must be coordinated through the Help Desk.**
- Unauthorized computers cannot be physically connected to the TMCC network and will be removed. This includes unauthorized wireless access points. **Impact: Rogue systems are not allowed on the TMCC network. Personal systems can connect to the public wireless where available.**
- Servers that are accessible from the Internet must be placed in a DMZ. This will require most access to TMCC networked resources to occur through the virtual private network (VPN). **Impact: Again, for now, users will have to log into <http://sag2.tmcc.edu> to access these resources.**
- Information on sensitive information technology hardware, software, and organizational information has been moved to move to a secure web site requiring authentication for access. **Impact: Sensitive information is only accessible after providing your username and password.**

Telephony Updates

Reiteration

- Do not move telephones from one location to another. They are not plug-and-play. These digital phones only work with the TMCC PBX and must be programmed for each location they are plugged into. If moving to another location or even within your current area, do not unplug the phone and move it yourself! Prior to moving the phone, the telephony team must retrieve valuable information in order to ensure the phone works properly in its new location; prematurely moving the phone will cause a delay in getting the phone working correctly. Contact the Help Desk if a phone needs to be moved.

Help Desk: Fiscal Year 2009 (July 2009 through June 2010)

1852 Total Requests/ 1800 Completed

- August 2009 Statistics (from August 1, 2009 through August 31, 2009):
 - 1076 recorded help desk requests (+300 from July 2009)
 - 1037 Completed =96.37%
 - Average Days to Complete Work Order = 2.66 (+0.08 from July 2009)
 - Email Viruses Blocked/Quarantined in August 2009: 271 = 0.02% of all email
 - SPAM Blocked in August 2009: 1,424,868 = 85.44% of all email
 - College-wide Computer Spyware/Adware and Other Viruses in August 2009:

§ Action	Viruses	Security Risks
§ Cleaned	0	0
§ Suspicious	0	0
§ Blocked	80	2
§ Quarantined	163	27
§ Deleted	0	16
§ Manually Repaired	24	9