



Truckee Meadows Community College

Information Technology Operations

Monthly Status Reports

• February 28, 2009

Network/Desktop Updates

- ITO has moved the Anti-Spam appliance into the DMZ (Demilitarized Zone) thus allowing you to safely manage your anti-spam settings from home or other remote locations.
- Occasionally, issues arise in the TMCC computing environment that TMCC faculty and staff should be made aware; however, pending a voice mail to everyone, there hasn't been a good way to communicate these issues. ITO has created a Splash page that will display on Windows-based systems after you have successfully logged in. It will only display if ITO needs to provide information about issues (i.e., problems with GroupWise, computer or network security issues, etc.).

Reiteration

- ITO Help Desk and the Software and Account management team has released a GroupWise security update (GroupWise hp1). This update corrects a serious security flaw the GroupWise email client. It is essential that all laptop users that have the GroupWise client installed on their laptops bring their laptops into the IT Operations Help Desk for servicing.
- 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.**
- Administrative and academic wireless networks will use WPA or higher encryption. **Impact: Older TMCC devices may require a newer wireless interface card.** For now, this does not impact the public wireless system.
- ITO Technical Support has updated the <http://www.tmcc.edu/security> web site with the following:
 1. Added a link to Symantec's Antivirus Daily Report that is updated constantly with the latest information on what to watch out for and what are the latest threats for home users.
 2. Added a link to the TMCC Telecommunications Policy and added information on the login screen that comes up on every computer.
- Academic Computing has upgraded presently supported Macintosh labs to Mac OS 10.5.5 in preparation to join supported Macintosh computers to the academic domain in order to support individual student login.
- Student Authentication was implemented in 2008; all students are now required to activate their student e-mail accounts and confirm login names and password are correct at <https://my.tmcc.edu/mytmcc/>.

Telephony Updates

- Six new 911 emergency poles have been installed outside and are operational at the following locations: the southeast corner of the IGT Applied Technology Center; the east parking lot adjacent to Meadowood South Building and the east parking lot adjacent to the Meadowood North Building; Red Mountain west parking area near Shipping and Receiving; the southeast corner of the E.L. Cord Child Care Center; the south parking circle near the Sierra Building. The installation of a seventh, solar-powered 911 tower is in progress at Parking Lot G, on the north side of the Sierra Building.

Reiteration

When you connect the voice mail system, you will need to use your default voice mail password to access your new voice mail mailbox. You can find detailed instructions on how to create greetings for your voice mail at <http://www.tmcc.edu/ito/telephony/voicemail/>. Voice mail messages can also be retrieved from outside of the college phone system by dialing 775-673-8200.

- 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 2008 (July 2008 through June 2009)

4529 Total Requests/ 4524 Completed

- February 2009 Statistics (from February 1, 2009 through February 28, 2009):
 - 764 recorded help desk requests (-24 from January 2009)
 - 764 Completed = 100%
 - Average Days to Complete Work Order = 4.16 (+1.79 from January 2009)
 - Email Viruses Blocked/Quarantined in February 2009: 109 = 0.001% of all email

- SPAM Blocked in February 2009: 1,387,055 = 85.32% of all email
- Individual Computer Spyware/Adware and Other Viruses in February 2009:
 - Dandini Campus: 543 Spyware/Adware and 21,287 Viruses
 - High Tech Center at Redfield = 0 Spyware/Adware and 4 Viruses
 - IGT Applied Technology Center: 5 Spyware/Adware and 53 Viruses
 - Meadowood Center = 369 Spyware/Adware and 711 Viruses