



Truckee Meadows Community College

Information Technology Operations

## Monthly Status Reports

April 30, 2009

### Network/Desktop Updates

- ITO Administrative Computing has inventoried and compiled a list of personal computers that are 5 years old and slotted for replacement.

### Reiteration

- 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....
- Academic Computing has implemented two new WEB-REB kiosks one has been placed in Vista building and the other in the ATC building.  
Academic Software Installation Request Form for FAL 2009 is now available on-line at <http://www.tmcc.edu/ito/downloads/forms/submit/softwarerequest/>
- 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.).
- 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.

## Telephony Updates

### Reiteration

- 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; th 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.
- 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)

### 5899 Total Requests/ 5896 Completed

- April 2009 Statistics (from April 1, 2009 through April 30, 2009):
  - 633 recorded help desk requests (-87 from March 2009)
  - 654 Completed = 1.03%
  - Average Days to Complete Work Order = 3.08 (+0.63 from March 2009)
  - Email Viruses Blocked/Quarantined in April 2009: 169 = 0.01% of all email
  - SPAM Blocked in April 2009: 1,535,806 = 87.78% of all email
  - Individual Computer Spyware/Adware and Other Viruses in April 2009:
    - Dandini Campus: 620 Spyware/Adware and 23,928 Viruses
    - High Tech Center at Redfield = 4 Spyware/Adware and 48 Viruses

- IGT Applied Technology Center: 0 Spyware/Adware and 4 Viruses
- Meadowood Center = 9 Spyware/Adware and 11,419 Viruses