



Truckee Meadows Community College

Information Technology Operations

Network Operational and Security Procedures

Following are procedures which apply to the security and operation of the TMCC computer network. Failure to follow these procedures is a violation of the TMCC Telecommunications Use Policy. Violations will be taken seriously and may result in disciplinary action, including possible termination. It is every employee's duty to use TMCC's computer resources responsibly, professionally, ethically and lawfully:

- 1) **Definitions:** From time to time in these procedures, we refer to terms that require definitions:
 - a) Computer Resources refers to TMCC's entire computer network. Specifically Computer Resources includes, but are not limited to: host computers, routers, switches, file servers, application servers, communication servers, mail servers, fax servers, Web servers, computer workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communications networks (for example, Internet, commercial online services, value-added networks, e-mail systems, that may be accessed directly or indirectly from the TMCC computer network).
 - b) Users refer to all employees, independent contractors, consultants, temporary workers, and other persons or entities that use our Computer Resources.
- 2) **Computer Resource Access:**
 - a) All Users of TMCC Computer Resources must first complete and submit a TMCC Application for Computer Systems Access form. The submission of this form is required to gain access to various TMCC Computer Resources and applications including email, mainframe and databases.
 - b) When an individual changes departments within TMCC or leaves the employment of TMCC, the TMCC Application for Computer Systems Access form must be submitted by the individual's supervisor/department to either change the access of the individual or request the individual's access be deleted.
- 3) **Physical Security:**
 - a) Prior to leaving computers unattended, Users are responsible for securing their computer workstation, preventing malicious users from gaining immediate access to TMCC Computer Resources.
 - b) When an individual leaves the employment of TMCC, the computer assigned to that individual will be reformatted prior to being assigned to another employee, thus eliminating the possibility that any personal information remains on the computer.
 - c) Computer room security is governed by the TMCC Computer Room Access policy.
- 4) **Network Security:**
 - a) Any devices connected to TMCC's network either through a direct Ethernet connection or wireless connection must have the device's Media Access Control (MAC) addresses registered with TMCC IT Operations. TMCC IT Operations will then set the IP address(es) that the device is allowed to use for access to the Internet or other TMCC Computer Resources.
 - b) Access to the TMCC network from a modem connection originating within a TMCC location (i.e., Dandini, Meadowood, Edison, Performing Arts Center, Redfield, etc.) is not allowed unless specifically established by TMCC IT Operations.
 - c) Computers on the TMCC network that must be accessed from an outside location must receive prior approval from TMCC IT Operations. TMCC IT Operations will establish the connection protocol that must be followed to access the internal computer from the outside. This is normally accomplished via a TMCC-provided virtual private network connection (VPN).
 - d) Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other Users by unnecessarily reviewing their files and e-mail.
 - e) A User's ability to connect to other computer systems through TMCC Computer Resources or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems or by appropriate TMCC authorities.

- f) Each User is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of TMCC's computer network. This duty includes taking reasonable precautions to prevent intruders from accessing TMCC Computer Resources without authorization and to prevent the introduction and spread of viruses. This is primarily accomplished by not circumventing and allowing:
 - i) Anti-virus programs to operate on and scan data on their computer workstations on a daily basis; and
 - ii) Security protocols issued by TMCC IT Operations and installed on their computer workstations to operate.
- g) Allowing malicious code to run on Computer Resources or broadcasting unregulated data traffic over the TMCC network is prohibited.
- h) Customers using the file transfer protocol (FTP) to transfer files to and from the TMCC network should recognize that FTP is not a secure method of file transfer.
- i) Remote access to and from TMCC computer workstations must be approved by IT Operations. Typically, remote access is strictly controlled for security reasons.
- j) Computers personally owned by TMCC employees (desktop computers, laptops, etc.) are not to be connected to the TMCC network since there is no guarantee the employee's systems are actively protected with the most current anti-virus or anti-spam signature files or have not been compromised by hackers.

5) **Wireless Network Security:**

- a) Wireless network connections are on an unprotected, shared network. Customers can use wireless networks at their own risk since wireless data traffic can be obtained by untrusted or unknown entities. Sensitive or confidential data must only be transmitted using wired networks. Since the wireless network is shared, it is more susceptible to viruses and other network attacks than the TMCC wired network and thus should be considered unreliable. Users of the wireless network must take every precaution to protect their devices from outside attacks. If problems occur on the wireless network, the network can be disconnected without notice at anytime and thus should be considered unreliable.
- b) Other than providing Internet access, direct access into TMCC Computer Resources via a wireless network is normally not allowed. Users must authenticate through provided security systems to gain authorized right to use TMCC Computer Resources.
- c) Wireless Access Points (WAPs) – Since wireless networks are inherently not secure, in order to ensure the security of the overall TMCC network, all WAP devices connected to the TMCC network must have their Media Access Control (MAC) addresses registered with TMCC IT Operations. IT Operations will set the IP address, the transmit power settings, and the radio channel the WAP is allowed to use for accessing the Internet or other TMCC network resources. However, if other TMCC-owned network devices are available for providing the same connectivity, the TMCC resources must be used.

6) **E-mail:**

- a) All e-mail messages processed by select NSHE mail servers will be subjected to an automated scanning process to (1) determine the likelihood that messages are spam and (2) detect viruses. Messages will be delivered, delivered with warnings, or rejected accordingly. Users following approved institutional procedures may have the opportunity to opt out of spam protection. Users may not opt out of virus scanning.
- b) Mail originating from a network address listed in the Domain Name Service Blackhole Lists (DNSbls) used by System Computing Services or TMCC will be rejected. No notification will be sent by TMCC to the intended recipient. No notification will be sent by TMCC to the sender.

7) **Virus Detection:**

- a) Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into TMCC's computer network. To that end, all material received on floppy or zip disk, flash drives, or other magnetic or optical medium and all materials downloaded from the Internet or from computers or networks that do not belong to TMCC must be scanned for viruses and other destructive programs before being placed onto the computer system. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to TMCC Computer Resources must be scanned for viruses.

- b) TMCC conducts virus scanning to reduce the number of viral attachments reaching TMCC users. Messages containing attachments are subjected to virus scanning and those determined to be viral will be rejected with an SMTP error. No notification will be sent by SCS to the intended recipient. No notification will be sent by TMCC to the sender. Such messages may be quarantined for further analysis. Potentially dangerous executable attachments (.ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .pif, .reg, .scr, .sct, .shb, .shs, .vb, .vbe, .vbs, .wsc, .wsf, and .wsh) and encrypted ZIP attachments containing such files may be rejected. All other attachments passing virus scanning will be delivered normally.
 - c) To prevent the automatic rejection of attached files, Users should send questionable file types (and request questionable file types be sent) in unencrypted ZIP attachments.
 - d) All computers including those from home Users connected to TMCC's administrative network must have the college's current anti-virus software installed, updated with the latest anti-virus signature and actively running.
 - e) If a Users desktop or laptop computer that is connected to TMCC Computer Resources gets infected, but does not have the college's current anti-virus software installed, updated with the latest anti-virus signature and actively running, the college is not responsible for fixing any problems that occur on the User's desktop or laptop computer as a result.
- 8) **SPAM:** Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send—most of the costs are paid for by the recipient or the carriers rather than by the sender. TMCC has an anti-SPAM filter in place to remove unwanted SPAM from the TMCC email system. However, not all SPAM is detected. If users receive unwanted SPAM in their inbox, forward the SPAM as an attachment to spam@tmcc.edu and request that the SPAM be filtered from future delivery.
- 9) **Passwords:**
- a) Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be written down, printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.
 - b) Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on their computer or on TMCC Computer Resources.
 - c) At no time will generic passwords be issued to allow multiple Users to use the same password for accessing TMCC Computer Resources.
 - d) Users are responsible for:
 - i) Changing their network password often. This should be done every two to three months. If Users suspect account tampering, Users should change their password immediately and report the tampering to TMCC IT Operations Help Desk by email or telephone.
 - ii) Making their password easy to remember but not easy for someone who may know them to guess (do not use birth dates, home phone numbers, favorite beverages, your dog's name, etc.)
 - iii) Choosing a password which is at least six (6) or more characters or digits long. User passwords should be a combination of alphanumeric characters (letters & numbers) and punctuation marks.
 - e) If Users allow others such as friends or colleagues to use their account, they are: i) Violating TMCC and NSHE policy ii) Responsible for any act that person might do while using the User's account. Users have a responsibility for their account and what happens with it.
- 10) **User Maintained Servers:** Users must inform TMCC IT Operations and TMCC Applications Development of any personal or college servers not maintained by TMCC IT staff. This includes servers hosting web pages that are linked to the TMCC web site. The information provided will include the physical location, IP address and MAC address of the server and the URL of any web pages originating from the server. This is to ensure the server receives appropriate Internet access and proper security patches and updates are applied. Whenever possible, web pages should be hosted on servers maintained by TMCC IT Operations and monitored by TMCC Applications Development.

11) Administrative Rights:

- a) Normally, faculty and staff at TMCC are provided with a computer in order to complete the tasks required for their job. The computer belongs to TMCC, not the individual employee, and is set up to ensure the primary software required for their job is configured and operating properly (i.e., email, word processing, spreadsheets, etc.). With the advent of current desktop operating systems, TMCC is able to ensure only authorized users log into TMCC Computer Resources. Normally, those using computers with the Windows operating system are given "Power User" rights. This allows the individual the ability to perform most common tasks, such as running applications, using local and network printers, changing desktop screensavers and wallpaper, and shutting down the computer. Typically, they can perform all functions necessary for doing their job. This may require requesting assistance from the computer Help Desk for loading software necessary for their job.
- b) Only the IT departments are typically allowed "administrative" rights. This is because a User with administrative rights has the ability to (1) modify the desktop operating system which can cause problems and (2) circumvent TMCC computer and network security controls. Too often, these are the primary causes of reduced productivity with a computer at the college. By not granting administrative rights, it helps the college enforce the TMCC Telecommunications Use policy by ensuring that individuals:
 - i) Cannot knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks;
 - ii) Cannot knowingly or carelessly run or install on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms
 - iii) Cannot violate terms of applicable software licensing agreements or copyright laws.
- c) Not granting administrative rights allows the college to ensure the software loaded on TMCC computers is compatible with current desktop operating systems.
- d) Convenience typically should not be enough of a reason for granting administrative rights. However, academic department chairs can request administrative rights be granted to an academic faculty member within their department by sending a request to the TMCC IT Operations Help Desk.
- e) If the User has been granted administrative rights, the User will have placed themselves at risk from either attacks from other computers (inside or outside of the network) or from problems caused by mismanagement of their own computer. In either case, since the faculty member now has administrative rights to their computer, it will be extremely difficult for IT Operations to troubleshoot the User's computer quickly if problems occur.
- f) If the User's computer is found to be the cause of problems on the TMCC network or if they have other problems caused by mismanagement of their own computer, the only recourse to TMCC IT Operations will be to shut down the User's computer system and restore it to the base image previously established for the model of computer in use. The faculty member should feel free to contact the TMCC IT Operations Help Desk to periodically update the base image of their computer to proactively assist with updates to their computer workstation.

12) **Physical Cables:** We do not allow network connection cables longer than 10 feet to be used on the network. Cables of this length cause network attenuation and connectivity problems. Eliminating long cables from the network keeps network traffic moving quickly and efficiently and eliminates unwanted "noise" on the network.

13) Backups:

- a) Daily incremental, weekly, monthly and annual transactions files backups will be made by TMCC IT Operations of all data that resides on servers managed and maintained by TMCC IT Operations. However, multimedia files (i.e., MP3, WAV, etc.) will be normally excluded from backups of servers or desktop computers.
- b) All data that resides on desktop workstations should have copies made quarterly of all master files and software necessary to restore and access the data for normal operations. Daily transaction files copies should be made. At least three copies should be made of all master and transaction files. One copy should remain in a secure area of the close to the desktop workstation under approved security procedures. One copy should be moved to the TMCC IT Operations Help Desk server under approved security procedures if storage space is available. If the application is critical, one copy should be moved to an off-site storage facility.