	Information Systems Technology Management Services	
	Name:	Workstation Use Policy
	Start Date:	01/06/2003
	Approval Date:	07/01/2021

Policy Body

Workstation Use Policy

Purpose: To describe guidelines concerning appropriate use and security of workstations, peripheral devices, protection of confidential information and securing unattended workstations to prevent unauthorized access.
Computer systems are a continually growing and changing resource that supports hundreds of users. These resources are vital for the fulfillment of the clinical and business needs of the Springfield Medical Care Systems organization. In order to ensure a reasonable and dependable level of service, it is essential that each individual exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt computer access for all users.

Scope: This policy applies to all users of SMCS, Inc and any authorized external entities.

Policy: Each employee shall be responsible for all computer transactions that are made with their User ID and password, and for the care and security of any computer or hardware assigned to them. Users shall not knowingly engage in any activity that may be harmful to any portion of the network, its data, or its users. Users shall take necessary precautions to protect confidential or sensitive information from inappropriate or unauthorized access by others, in accordance with practice policies.

Procedures and Guidelines: The following guidelines govern the appropriate use of computer systems. Because it is impossible to anticipate all the ways in which individuals may misuse these resources, this policy focuses on a few general rules and the principles behind them.

Workstation Use:

1. All users that have been granted access to computer systems are accountable for their activity and use. SMCS is the sole owner of all computer equipment. The data files therein, are the sole property of the institution, and may be viewed by Administration if deemed necessary.
2. All users are expected to utilize the computer systems in a responsible manner which is consistent with Springfield Medical Care Systems polices and guidelines.

Workstation Access: The Technology Management Services department will review and assign the level of access granted to users as required.

1. The standard level of access on a Windows computer account will be "Restricted User" level. This will ensure users cannot install software on computer systems.
2. The privilege level of a user's windows computer account will be increased to the "Administrator" level only to allow for the functionality of non-standard software. The

Technology Management Services department will document all such authorizations.

3. Each user will be given a unique login. The use of group credentials is prohibited.
4. Users should be aware that the Technology Management Services Department provides and preserves the security of files; account numbers, and passwords, security can be breached through actions or causes beyond our reasonable control. Users are responsible for use of their computer accounts and system access and must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their account by unauthorized persons. Please refer to the Password Management Policy for complete details.

Unauthorized Workstation Use: The following activities are prohibited**.**

1. Installation or use of software including, but not limited to games, web browsers, instant messaging, chat programs, music and personal picture files is prohibited. Software required for end user use must be approved and installed by Technology Management Services staff only.
2. The use of computer systems irresponsibly or in a manner that unreasonably and adversely affects the use of these resources by others. This includes intentionally, recklessly or negligently damaging any system by the introduction of any so-called "virus", "worm", ·spyware", or "trojan-horse" program.
3. Use of computer systems for non- business related activities that unduly increase network load (e.g., music, video, chain mail, network games and spamming) is prohibited.
4. Use of an account for purposes unrelated to the objectives for which the account was issued is prohibited.
5. Users are prohibited from storing or saving ePHI or sensitive information on their local workstations. Users are required to save ePHI or sensitive information to the file server on the network.
6. Authorized computers only are allowed on the Springfield Medical Care Systems networks. Users may not attempt to gain access to the network with personal computer / electronic devices of any kind. For remote access please refer to the Remote Access policy. Users may not install hardware of any kind into workstations such as but not limited to memory sticks, network cards, wireless usb devices, mp3 players, cell phones and cameras. All hardware components must be approved and installed by Technology Management Services staff only.
7. Users may not install network devices on the network of any kind including, but not limited to, routers, switches, hubs, wireless access points, network hard drives, or printers.
8. Bypassing, subverting or otherwise rendering ineffective the security or access control measures on any computer or network is prohibited.
9. The use of software programs that illicitly examines or obtains user accounts, local computer accounts, network accounts, passwords, IP addresses, network information, software, files or any SMCS resources is prohibited.
10. Use of false or misleading information for the purpose of obtaining access to unauthorized resources is prohibited.
11. Users may not intentionally disrupt or damage Springfield Medical Care Systems computers or networks in any way.
12. Accessing, altering, copying, moving, or removing Organizational Data, proprietary software or other files (including programs, libraries, data, patient health information and electronic mail) from any network system or files of other users without prior authorization is prohibited.
13. Using computer systems for one's own commercial gain or for any other commercial purposes not approved by management is prohibited.
14. Saving files to any location other that SMCS or Hospital owned Network is prohibited unless explicitly approved. File share programs such as google docs etc, are not permitted as

they can't be audited or monitored.
15. Using SMCS or Hospital equipment to save personal files outside our environment is prohibited.

Physical Access and Security: Users are responsible for the physical security of and access to hardware, software, and data entrusted to their use. The following practices should be followed.

1. All users are required to logoff or lock their computers when the computer will be unattended by pressing the ctrl-alt-del keys and then press the "lock computer" button.
2. All workstations will have an automatic time out of 15 minutes of no use.
3. Workstations that cannot be protected from public view must have privacy screens.
4. Laptops and mobile devices which access patient health information or sensitive business information should be physically secured when not in use. The equipment should be locked in a closet, office or desk when not in use.
5. Department Managers should request computer moves and network-related changes through the Technology Management Services Help Desk.
6. Anti-virus software will be installed on all computer workstations, according to the "standard build" and will be configured to receive anti-virus definition updates.
7. Virus and vulnerability scans are run on a periodic basis on all SMCS supported machines. Users that are authorized to use any form of removable media should perform a "virus check" that have not been under their personal control in their work area, before using the contents on their computers.
8. Users who get a message from the virus scanning program that it was unable to clean a virus or the files have been quarantined should stop using the contaminated computer, and contact the Help Desk.
9. Workstations are configured to receive Microsoft critical updates in a timely manner. Operating systems which are no longer secure due to obsolescence (and therefore no longer have security updates made available to fix vulnerabilities), should be upgraded to a currently supported version by the Technology Management Services department.
10. As new laptops and tablet computers which access patient health information or sensitive business information are added to the network environment, whole disk encryption software will be installed.
11. Computer operating system firewalls are enabled.
12. Systems that are not installed and maintained by the Technology Management Services Department are required to be maintained at the same levels of protection as SMCS devices (e.g. vendor equipment).

Internet Use and Restrictions: Springfield Medical Care Systems utilizes software that can track and block internet access. Internet site categories that are deemed a security or productivity liability will be blocked on a global basis. Department managers can identify specific workstations to be denied access to any Internet site outside of a limited white list. Department managers can request an audit of the internet activity of any specific workstation or user. When using the internet, users should adhere to all relevant Technology Management Services and organizational policies. The following practices should be followed:

1. Utilization of computer resources in general and internet practices in particular should adhere to professional conduct standards. Violations would include accessing or propagating illegal, obscene, confidential, libel or harassing material.
2. Downloading electronic files such as music, screen savers, desktop wallpapers and shareware is prohibited.
3. Downloading software must be done through the Technology Management Services Department.

4. Users are prohibited from accessing web sites that depict or espouse pornography, hatred, bigotry or violence. Users found doing so are subject to disciplinary action.
5. Users are prohibited from sharing their Internet access accounts or passwords.
6. Users are prohibited from surfing the internet casually at the expense of work productivity. Access to the internet is granted to individuals and is for business use only.
7. Users are prohibited from replacing the browser or modify Internet access in any way. Doing so defeats proper and secure functioning of access set up.
8. Users have the responsibility to promptly report any violation of this policy. In addition, users must report any information relating to a flaw in or bypass of a computer systems security measure to the Director of Technology Management Services.
9. While SMCS desires to maintain user privacy and to avoid the unnecessary interruption of user activities, SMCS reserves the right to investigate unauthorized or improper use of computer systems, which may include the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to SMCS policy or applicable law, appropriate measures will be taken.

Interpretation

1. The examples of unauthorized use set forth above are not meant to be exhaustive. If a user is in doubt regarding an issue of questionable use, please contact your manager or the Director of Technology Management Services. Additional questions about this policy or of the applicability of this policy to a particular situation should be referred to the Director of Technology Management Services. The Technology Management Services department is the final authority on questions of appropriate use of SMCS resources.

By signing below I acknowledge that I read and understand the Work Station Use policies and procedures.

Signature: _____ Date:_____

Printed Name:_____

Document Link Manager

No Documents Linked No Documents Linked

Attachment Manager

Attachments List:

Name	Size
Top Ten Security Tips.ppt	647 KB
Top Ten Security Tips.doc	54 KB