ACCEPTABLE USE POLICY FOR COMPUTERS & NETWORK RESOURCES

Revision 08.31.18

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Sleep Medicine of America, LLC or Sleep Centers of Middle Tennessee, PLLC (hereinafter "SCMT") in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

SCMT provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

Scope

All employees, contractors, consultants, temporary and other workers at SCMT, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by SCMT, or to devices that connect to an SCMT network or reside at an SCMT site.

Exceptions to this policy must be approved in advance by the Practice Administrator.

Policy Statement

1. General Requirements
   1.1. You are responsible for exercising good judgment regarding appropriate use of SCMT resources in accordance with SCMT policies, standards, and guidelines. SCMT resources may not be used for any unlawful or prohibited purpose.

   1.2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic. Devices that interfere with other devices or users on the SCMT network may be disconnected. SCMT prohibits actively blocking authorized audit or virus scans. Firewalls and other blocking technologies must permit access to the scan sources.

2. System Accounts
   2.1. You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
   2.2. You must maintain system-level (generally computer) and user-level (generally application) passwords in accordance with system-enforced password rules.

   2.3. You must ensure through legal or technical means that proprietary information remains within the control of SCMT at all times. Conducting SCMT business that results in the storage of proprietary information on personal or non-SCMT controlled environments, including devices

maintained by a third party with whom SCMT does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by SCMT, or its customer and partners, for company business.

3. Computing Assets
   3.1. You are responsible for ensuring the protection of assigned SCMT assets. Promptly report any theft of SCMT assets to the Practice Administrator.

   3.2. All PCs, tablets, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

   3.3. Do not interfere with corporate device management or security system software.

4. Network Use
   You are responsible for the security and appropriate use of SCMT network resources under your control. Using SCMT resources for the following is strictly prohibited:

   4.1. Causing a security breach to SCMT network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

   4.2. Causing a disruption of service to SCMT network resources, including, but not limited to, streaming music, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

   4.3. Downloading or viewing pornography or sexual content.

   4.4. Downloading games or playing online games of any kind.

   4.5. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

   4.6. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

   4.7. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

5. Electronic Communications
   The following are strictly prohibited:

   5.1. Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates SCMT policies against harassment or the safeguarding of confidential or proprietary information.

   5.2. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

5.3. Sending pornography via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication. Any pornography received via electronic communications should be reported and deleted.

5.4. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

5.5. Use of a SCMT e-mail or IP address to engage in conduct that violates SCMT policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a SCMT e-mail or IP address represents SCMT to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with SCMT.

NEW HIRES

THIS COPY IS FOR REFERENCE ONLY

PLEASE USE LINK IN SCMT'S EMPLOYEE PORTAL TO SIGN THIS FORM DIGITALLY AFTER YOU HAVE FINISHED REVIEWING ALL DOCUMENTS