medicine·on·time®
BE INDISPENSABLE™

Medicine-On-Time (MOT)

Information Technology Policy

1. **Purpose:**

1.1. The purpose of this document is to establish and define the framework by which the company will maintain general IT Controls, policies and procedures.

1.2. To be effective, information security must be a team effort involving the participation and support of every MOT employee who deals with MOT data. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the behavior needed to protect MOT information. This document describes ways to prevent and respond to a variety of threats including unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of MOT data.

1.3. Information is essential input to all of the work that MOT performs. As a result, information security has become a critical factor in the production of MOT's products and services. In recognition of this fact, the Information Technology department acts as MOT's focal point for all information security issues. Specific questions about the policies described here can be directed to the Help Desk or the manager within your department.

2. **Scope:**

2.1. This policy statement applies to all computer and data communication systems owned by and/or administered by MOT. The document covers only information handled via computers and/or networks. Although the document includes mention of other manifestations such as voice and paper, it does not directly address the security of information in these forms.

2.2. This policy statement applies to all employees, contractors, consultants, temporaries, and other workers at MOT, including those workers affiliated with third parties who access MOT computer networks. Throughout this policy, the word "user" will be used to collectively refer to all such individuals.

3. **Attachments:**

3.1. none

4. **Policy:**

4.1. The VP of IT (or senior management official with responsibility for IT), will establish a framework of clearly defined policies and procedures for the daily operation and management of the company's IT infrastructure and application base. They will ensure that all employees, contractors, consultants and vendors interacting with IT shall know, and their actions shall be guided by, these procedures.

4.2. Under no circumstances is an employee of MOT authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing MOT-owned resources.

4.3. System Access Control

4.3.1. Signed Forms Required for Issuance of User ID

4.3.1.1. Prior to being given an enabled user ID allowing access to MOT systems, the following must be completed:

4.3.1.1.1. MOT New Hire Setup request is submitted by an employee's manager and approved by the Senior VP of IT.

4.3.1.1.2. General IT Controls Policy (this document) signed by the employee.

4.3.1.1.3. MOT Confidentiality and Non-Compete Agreement (available from Human Resources) signed by the employee.

4.3.2. Authorization

4.3.2.1. To comply with the MOT General IT Controls Policy users are required to get authorization for system access. The Information Technology department is responsible for maintaining a record of these authorizations. Contact the Help Desk to receive proper authorization.

4.3.2.2. The human resources department is responsible for notifying the IT administrators when an employee resigns or is terminated. Upon notification the IT administrator will execute the Standard Operating Procedures for deactivating user accounts.

4.3.3. Passwords

4.3.3.1. The length of passwords is verified by the system at the time that users create them. All passwords must have at least eight characters, at least one of which is numeric.

4.3.3.2. All user-chosen passwords for computers and networks must be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "12345678" must not be employed.

4.3.3.3. Passwords must not be written down and left in a place where unauthorized persons might discover them.

4.3.3.4. Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user, the Help Desk, or a System Administrator. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use public directories on local area network servers, and other mechanisms.

4.3.4. Responsibility

4.3.4.1. Users are responsible for all activity performed with their personal user-IDs. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their user-IDs. Similarly, users are forbidden from performing any activity with IDs belonging to other users (excepting anonymous user-IDs like "guest").

4.3.4.2. If the computer system to which a user is connected contains sensitive, valuable information, or administrative access, they must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out or locking the system.

4.3.4.3. Users must not read, modify, delete, or copy a file belonging to another user without first obtaining permission from the owner of the file. Unless general user access is clearly provided, the ability to read, modify, delete, or copy a file belonging to another user does not imply permission to actually perform these activities.

4.3.4.4. Users using MOT systems are prohibited from gaining unauthorized access to any other Information System or in any way damaging, altering, disrupting the operations, or creating denial of service of these systems. Likewise, users are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access.

4.3.4.5. Users must promptly report all information security alerts, warnings, suspected vulnerabilities, and the like to the Help Desk. Users are prohibited from utilizing MOT systems to forward such information to other users, whether the other users are internal or external to MOT.

4.4. Computer System Use

4.4.1. Ownership and Privacy

4.4.1.1. Computer systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, email, WWW browsing, and Instant Messenger, are the property of MOT. Use of computers, as with other company assets, should be limited to situations related to work assignments. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

4.4.1.2. While MOT's administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of MOT. Because of the need to protect MOT's network, management cannot guarantee the confidentiality of information stored on any network device belonging to MOT. MOT employees shall have no expectation of privacy in anything they store, send or receive on the company's systems. Furthermore, although it is not obliged to monitor email content, MOT reserves the right to monitor such messages without prior notice.

4.4.1.3. Employees, temporaries, contractors, and consultants must return all hardware, software, working materials, confidential information, and other property belonging to MOT upon termination.

4.4.2. Restrictions of Use

4.4.2.1. Users must not post, duplicate, or distribute files, code, executables, or other information in public areas such as newsgroups, web pages, and bulletin boards that contain proprietary product, development, or personnel information that is the property of MOT.

4.4.2.2. Users must not make fraudulent offers of products, items, or services originating from any MOT account.

4.4.2.3. Using a MOT computing asset to actively engage in activities that is in violation of harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited. MOT retains the right to remove from its systems any material it views as offensive or potentially illegal and to take appropriate action where appropriate.

4.4.2.4. Users may not use computer or network resources to retrieve, share, or distribute material that is protected by copyright. This includes and is not limited to software, music, videos, and movies. . Systems administrators reserve the right to remove such information and software unless authorization from the rightful owner(s) can be provided by the involved users.

4.4.2.5. Use of point-to-point file sharing programs (e.g., Kazaa, Morpheus, BitTorrent, Grokster, etc.) is prohibited.

4.4.2.6. Games may not be installed on any MOT computer systems. Games included with the operating system that are loaded by default are exempt.

4.4.2.7. Users must not intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is known as a virus,, worm, Trojan horse, spyware, rootkit, bot, bug and similar names.

4.4.2.8. Instant Messaging applications including AOL, ICQ, MSN, Yahoo, Trillian, and Skype are permitted for use. Other Instant messaging solutions require approval from Information Technology. Support for these applications will not be provided by the MOT IT staff or Help Desk. Instant Messenger use is a privilege and will be monitored for abuse. Excessive or inappropriate use of Instant Messaging will not be tolerated.

4.4.2.9. MOT management encourages workers to use the Internet. If Internet use is for personal purposes, it must be done on personal, not company time. Likewise, news groups, discussion groups, games, and other activities which cannot definitively be linked to an individual's job duties must be performed on personal, not company time. If a manager determines that users are abusing Internet privileges the access can be revoked and lead to disciplinary action up to and including termination.

4.5. MOT Remote Network access

4.5.1. Third party vendors must be verified as an authentic entity (ie. IT help desk, systems administrator, etc.) before allowing remote access to Company's computers and networks, and only be given in-bound remote maintenance privileges when the system administrator determines that they have legitimate business need. These privileges must be enabled only for the time period required to accomplish approved tasks and restricted to the resources needed to accomplish their task.

4.5.2. Information regarding access to MOT computer and communication systems, such as router phone numbers, is considered confidential. This information must NOT be posted on electronic bulletin boards, listed in telephone directories, placed on business cards, or otherwise made available to third parties without authorization from an Information Technology administrator. Fax numbers, and email addresses are permissible exceptions to this policy.

4.5.3. Employees are prohibited from installing remote control software on workstations which are simultaneously connected to a local area network (LAN) or another internal communication network without authorization from an Information Technology Administrator.

4.6. Software, Media & Storage Devices

4.6.1. To assure compliance with in-house information security standards, all software and software licenses must be procured through Information Technology.

4.6.2. MOT strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If users make unauthorized copies of software, data, or content the users are doing so on their own behalf, since all such copying is strictly forbidden by MOT. Likewise, MOT allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of the author/owner.

4.6.3. To help prevent unauthorized duplication all media and licenses of a software product that is being discarded must be physically destroyed before it can be placed in the garbage.

4.6.4. Any device that could possibly store data or software must first be destroyed such that information is irretrievable before it can be placed in the garbage.

4.7. Phone Systems

4.7.1. Internal phone lists must not be distributed outside the company without specific authorization of a department manager. Contractors, consultants, temporaries and other third parties working for MOT may, of course, have phone directories if necessary to perform their jobs.

4.7.2. Telephones are provided to facilitate business activities. Telephones must not be used for personal purposes, unless the calls cannot be made during off-business hours. In these cases, the personal calls must be kept to a reasonable length.

4.8. Wireless Access

4.8.1. Devices that provide wireless access to computer networks are provided by and maintained by the Information Technology department. Under no circumstance shall anyone besides Information Technology connect or power on a wireless access point, even if the device is not connected to any internal network.

4.8.2. Users are granted access to the guest wireless network that is provided. Information Technology will follow the standard operating procedure for adding users for secure wireless connections.

5. Procedure:

5.1. General IT Controls Agreement

5.1.1. It is the responsibility of users to comply with all information security policies and procedures. When the undersigned is hired, he/she acknowledges that he/she is a "user" as defined in section 2.2. As a user, the undersigned additionally acknowledges that he/she must comply with the security measures dictated by MOT as defined in this General IT Controls procedure.

5.1.2. As a user, the undersigned acknowledges that he/she is a fiduciary in possession of MOT information resources. This means that the undersigned must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

5.1.3. The undersigned acknowledges that he/she has read this MOT General IT Controls procedure and understands the policies and procedures described therein. The undersigned agrees to abide by the policies and procedures described therein as a condition of continued employment. The undersigned furthermore understands that violators of these policies and procedures are subject to disciplinary measures including privilege revocation and/or employment termination. The undersigned understands that access to MOT Information Systems is a privilege which may be changed or revoked at the sole discretion of MOT management, and which automatically terminates upon departure from MOT.

5.1.4. The undersigned certifies that he/she has received a copy of this document for future reference. The undersigned also understands that changes and updates can be made to the General IT Controls procedure, and that all users will be notified when of such changes. The undersigned agrees to review updates and changes of future releases of this General IT Controls procedure.

User's signature and today's date

User's name (print)

----

6. **Evidence**

6.1. Evidence of these policies and procedures can be viewed in the control binder located in the VP of IT’s office.

6.2. Evidence of temporary employees, contractors and consultants recognition of corporate policies and procedures can be obtained through the VP of IT.