M2S

Approved

Systems Security Policy and User Guidelines

This policy pertains to use of ***M2S Computer and Network Systems***. These systems are to be used for business purposes in serving the interests of the company in the course of normal operations. Internet access is provided by M2S to assist employees in obtaining work-related data and technology.

All data that is composed, transmitted, or received via our computer communications systems is part of the official records of M2S and, as such, is subject to disclosure to law enforcement or other third parties. Therefore, employees should always ensure that business information contained in e-mail messages and other transmissions is accurate, appropriate, ethical, and lawful.

M2S reserves the right to audit equipment, networks and systems, including internet and email usage, to ensure compliance with this policy.

Abuse of M2S computers and network systems, including the internet, in violation of law or M2S policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy.

M2S prohibits the use of computers and network systems in ways that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

Integrity of Computer and Network Systems

1. M2S complies with all hardware and software licensing agreements. Report any violations to your supervisor and IT.

2. All M2S employees must keep their passwords secure. If you suspect that an account or password has been compromised, report the incident to IT.

    a. Do not include passwords in email messages or other forms of electronic communication.

    b. Passwords are not to be given to anyone else, except the system administrator, for any reason. This includes family or other household members when work is being done at home.

3. All computers must be secured with a password-protected screensaver with automatic activation set at 15 minutes or less, or by logging off when the computer will be unattended.

4. Virus Prevention:

    a. No USB flash drives shall be inserted or mounted without a virus scan.
    b. CDs or DVD's of home or unknown origin are not to be inserted or mounted by M2S equipment.

5. Because information contained on laptop computers is especially vulnerable, special care shall be exercised and users of this equipment shall have specialized training.

6. If equipment or systems need repair or maintenance, send an email to Help@m2s.com or call the Help Desk at extension 400.

The following activities are strictly prohibited:

1. The installation of any unapproved software or hardware is strictly prohibited unless approved by IT.

    a. Please see the Approved Workstation Software document for a list of approved software.

2. The use of personal equipment not limited to but including items such as computers, laptops, and USB storage devices in secure areas of the buildings are strictly prohibited.

    a. Visitors and guests may use personal computers on the guest network only within designated areas such as training and conference rooms unless authorized by a member of the IT group.

3. Connecting a personal computer or other non-M2S computer to the M2S network via physical or VPN connections unless prior authorization from the IT Manager. (Wireless access will be provided for visitor's non-M2S computers in limited locations.)

4. Using M2S email addresses and systems for personal use. (M2S users should use a "Hotmail" or "Yahoo" email account for such purposes.)

5. Hacking (unauthorized use of computer and network resources).

6. Sending spam, including chain letters, solicitations, or advertisements not related to business purposes or activities.

7. Harassment of anyone via email, telephone or paging, whether through language, frequency, or size of messages.

8. The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet.

9. Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions.

10. The utilization of M2S VPN solutions on non-M2S equipment without prior approval from the IT Manager.

11. Copying, distributing, and or sharing of any purchase license software without prior authorization from the IT manager.

Storage of Electronic Patient Health Information (PHI)

Technical Safeguards

Access Control

1. All M2S electronic devices, which send, receive, manage or maintain PHI for Designated Health Care Components shall comply with all M2S HIPAA policies.

Password Protection

1. When employees with access to PHI are away from their computers for extended periods, the computer station shall be secured with a password protected return from sleep or screen saver feature.
2. No computer that contains access to PHI shall remain logged on outside of an employee's office hours or when the work station is temporarily vacated.
3. Laptops, handheld PDA's, smartphones and cell phones, which contain PHI shall be locked and/or secured at all times and should not be accessible without password entry.
4. Laptops, handheld devices, storage media (backup drives, CDs, DVDs, zip drives or external hard drives) shall not be left unattended,

should be fully secured and must remain password protected at all times.

5. In the event that a M2S owned laptop or other portable electronic device used by a designated employee, including backup drives, which contain PHI is removed from M2S property, the device shall maintain password protected and encryption at all times.

Transmission Security

1. ePHI shall only be transmitted using approved secure electronic messaging, including encryption and a secure transmission line.
2. All attachments transmitting PHI electronically shall be password protected and encrypted.
3. Prior to sending an electronic transmission of ePHI, addresses of all recipients shall be carefully verified to avoid communication misdirection.
4. Personal e-mail accounts (e.g. AOL, Gmail, Yahoo, Hotmail) shall never be used to conduct business.
5. **The communication of PHI and or attachments containing PHI via email is strictly prohibited.**
6. **The communication or sharing of confidential information, PHI or trial sensitive information via other electronic communication, including social media, is strictly prohibited. This may include but is not limited to: Facebook, Linked In, Google+ and Twitter.**
7. **The storage of confidential information, PHI or trial sensitive information via external storage or services that is not explicitly approved for such purposes is strictly prohibited.**
8. If an employee believes that sensitive data has been compromised in any manner, the employee shall immediately notify the Security Officer or Manager.

ePHI Storage

1. M2S staff must not create, store, access, transmit or receive ePHI on personally owned computers.

2. Employees who require remote access to company workstations or systems that hold ePHI must use a M2S-provided, fully managed device, and they must log-in via a Virtual Private Network connection.

3. You must securely destroy or delete ePHI when no longer needed or when retiring computers, smartphones or other mobile devices such as thumb drives.

4. All ePHI data shall be permanently stored in designated repository and systems as determined by the IT department. The systems listed in ePHI Server Control List SEC-WRK-0-03 have been approved for permanent ePHI storage.

Note: System such as Dacserver only process transient data and should not be considered for permanent storage. Any additional systems must be approved by IT prior to storing ePHI.