

## **OVERVIEW**

Company owned computers including desktops and laptops, phones, and tablets are to be configured, secured and encrypted by the IT Manager or an assigned technical support professional.

It is every associate of Amerimed's responsibility to protect our tablets and computer systems from damage, loss, theft, and unauthorized access and/or use. Laws and penalties have been put in place by the States to protect personal and corporate owned computer systems and networks from unauthorized access and alterations such as unauthorized installation of software, unauthorized removal of software and unauthorized alteration of configurations.

## **SECTION A**

### **Unauthorized Access and Alterations**

"Unauthorized access" entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent. These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks.

## **SECTION B**

### **Remote Access**

"Remote access" is a feature utilized by both internal and contracted technical support staff. Remote access of any company computer and/or tablet is strictly prohibited unless authorized by the IT Manager or the OCE. In the event of an emergency technical breakdown and the IT Manager cannot be reached, employees are to contact the appropriate manager according to the Daily Operations, Reference Guide.

## **SECTION C**

### **Company Owned Devices - Assigned**

Employees in an administrative, supervisory, or management position may be provided with one or more company owned electronic devices. Such employees must exclusively use assigned devices to conduct company related business. Care should be taken to prevent damage, loss, theft, or unauthorized use of all assigned devices, and any issues should be immediately reported to IT Management and/or Support Services. Assigned devices remain property of Amerimed and must be surrendered upon request, and returned immediately if employment ends.

### **Company Owned Devices - Shared**

Often associates are tasked with performing duties on computers or electronic devices that are not explicitly assigned to them. These "shared" devices can be found in use for ambulance and MIH crews, PC's for use by Shift Commanders and other crew leaders, shared PC located in Amerimed stations for use in clocking in/out and/or performing required daily duties, and occasional other situations. Shared devices are subject to specific policies about the use of shared accounts and

restricted from adding any personal accounts or software. These important guidelines need to be followed to ensure a) security of employee information, b) IT system security, and c) HIPAA compliance and protection of any protected patient information.

Detailed company policies for access and use of all corporate owned electronic systems and accounts can be found at **1.5.1 Electronic Systems & Corporate Accounts**

## **SECTION D**

### **Personal Electronic Devices**

Due to the significant risk of harm to the company's electronic resources, or loss of data, from any unauthorized access that causes data loss or disruption, employees shall not bring personal computers or data storage devices (External hard drives, USB / flash drives, "smart" phones, iPads or similar devices, laptops or other mobile computing devices, or other data storage media) to the workplace and connect them to company electronic systems unless expressly permitted to do by the IT Manager or OCE.

The use of personal devices for any business-related work, including handling of any patient-related documentation, is strictly prohibited. Devices outside of the company's control and management could constitute violations of HIPAA and can also nullify your right to privacy of your personal information and data.

For those rare instances an associate has authorization, to minimize the risk of unauthorized copying of confidential company business records and proprietary information that is not available to the general public, any employee connecting any above mentioned device to company networks or information systems thereby gives permission to the company to inspect the device at any time with personnel and/or electronic resources of the company's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential company business records and proprietary information have not been taken without authorization.

Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to company computers or networks.

## **SECTION E**

### **Pertinent Regulations**

*Computer theft:* Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

1. Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession;
2. Obtaining property by any deceitful means or artful practice; or
3. Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property shall be guilty of the crime of computer theft.

*Computer Trespass:* Any person who uses a computer or computer network with knowledge that such use is without authority and with the intention of:

1. Deleting or in any way removing, either temporarily or permanently, any computer program or data from a computer or computer network;
2. Obstructing, interrupting, or in any way interfering with the use of a computer program or data; or
3. Altering, damaging, or in any way causing the malfunction of a computer, computer network, or computer program, regardless of how long the alteration, damage, or malfunction persists shall be guilty of the crime of computer trespass.

*Computer Invasion of Privacy:* Any person who uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is without authority shall be guilty of the crime of computer invasion of privacy.

*Computer Forgery:* Any person who creates, alters, or deletes any data contained in any computer or computer network, who, if such person had created, altered, or deleted a tangible document or instrument would have committed forgery under Article 1 of this chapter, shall be guilty of the crime of computer forgery. The absence of a tangible writing directly created or altered by the offender shall not be a defense to the crime of computer forgery if a creation, alteration, or deletion of data was involved in lieu of a tangible document or instrument.

*Computer Password Disclosure:* Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of \$500.00 shall be guilty of the crime of computer password disclosure.

*Criminal Penalties:* Any person convicted of the crime of computer theft, computer trespass, computer invasion of privacy, or computer forgery shall be fined not more than \$50,000.00 or imprisoned not more than 15 years, or both.

Any person convicted of computer password disclosure shall be fined not more than \$5,000.00 or incarcerated for a period not to exceed one year, or both.