AMERIMED SOP
1.5.1 Electronic Systems & Corporate Accounts
Rev 5/2024

OVERVIEW

Company electronic systems and corporate accounts are the infrastructure of every administrative and operational process. Protecting the integrity of both must be the highest priority of every Amerimed associate.

SECTION A

Electronic Systems

Company owned electronic systems and networks include but are not limited to: computers, tablets, fax machines, cell phones, 2-way radios, telephone systems, GPS and WIFI devices, access points, hotspots, etc, and all other forms of Internet/intranet access, remote access, server access, and VPN's, storage mechanisms such as internal and external hard drives, portable storage devices such as USB drives and media cards including those inserted into company owned cell phones, and cloud storage such as OneDrive, SharePoint, etc.

Internet

For security and quality-of-use reasons, any stationary desktop computer devices should be connected to the internet via a wired Ethernet connect. Wi-fi connections are not to be used as permanent internet connections for computers or printers at Amerimed facilities.

The use of wi-fi from inside the facilities should be limited to

- Devices that are company-owned and are intended to be portable and mobile. (Tablets, laptops, phones assigned to an employee or vehicle);
- Guests such as vendors who may require a wi-fi connection to do business while on site;
- Specific devices that may not be able to connect via wi-fi but are not used for public access to the internet (permanently installed security cameras, etc);

Unless specifically granted in this policy, or permission granted by the IT Manager or the OCE, any non-business use of the company's electronic systems is expressly forbidden.

SECTION B

Corporate Accounts

The company maintains corporate accounts for all business software and applications that are needed for the operation of business. Account user information is administered by management including the IT Manager, VPs, General Managers, Area Managers, and Division Managers. User credentials are issued for the sole use of the associate to which they are assigned, and should never be shared with others unless in an official capacity.

Corporate accounts include but are not limited to: accounts used to set up, monitor, communicate through, and/or allow access to applications, software, data files, electronic patient care reports, employment systems, email systems, remote access, vendor accounts, computers, tablets, cell phones, and any other electronic system wherein the user must log into the account to use the application, software, access data, files, cloud storage, etc. and/or use the device. Examples of the

corporate accounts that the company maintains are Microsoft, Traumasoft, Adobe, NetSuite, Paycom, BambooHR, eFax, and others.

No associate is authorized to open any new account with any software vendor, online or otherwise, without the express permission of the IT Manager and/or OCE.

SECTION C

File Storage

The company utilizes online ("cloud") based systems for all key operating systems and applications. This includes file storage utilizing OneDrive and SharePoint to store all documents in online databases. Cloud storage provides HIPAA-compliant security, backup redundancy, portability, and better organization of important files and documents. All company-owned devices including desktop PCs, laptops, tablets, etc., should be configured to utilize our cloud-based storage systems. No files should ever be maintained exclusively on an individual devices "hard drive" or on an external drive, in order to prevent loss damage to the information.

SECTION D

Shared Computer Use Policies

In cases where computer devices are to be shared among multiple users, there are important guidelines that 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.
With these shared computers, these guidelines should be followed at all times:

- Never add any personal accounts or logins to this computer. This includes things like personal email addresses, Google or Microsoft accounts, i-Cloud, stored profiles in web browsers etc. Do not add additional "profiles" to web browsers or the Windows system.
- Never download or add any additional software to a shared PC without specific authorization. Most importantly, anti-virus software like McAfee or Norton is sometimes offered when accessing other programs. These programs can create serious issues on our systems and should never be on any Amerimed computer.
- Only web-based email should be used. (Accessed through amerimed.net/webmail) If the webmail asks to "remember" or "save" information for future use, this should be declined. This is to prevent others from easily accessing others company email accounts. Users should always log out of email accounts when leaving the shared computer. Installed email software like Outlook should not be used on shared computers.
- If using Microsoft Teams, individual users should enter via the online "web" version. (Found at microsoft.com/en-us/microsoft-teams/log-in). Users should log out when the session is finished to prevent unauthorized access.
- On crew devices like Toughbooks, never save or store any photo or document containing protected patient information (Face sheets, narratives, etc.) If they are captured or scanned to be uploaded into the Traumasoft ePCR, the files must be immediately deleted from the computer and the Recycle Bin emptied to prevent unauthorized access

SECTION E

General Usage

Brief and occasional personal use of the electronic systems and/or accounts is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the company or otherwise violate this policy. (See “No Expectation of Privacy” below)

Electronic communication should not be used to solicit or sell products or services that are unrelated to the company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of company owned electronic systems and accounts as defined above is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate company purposes;
- • Engaging in private or personal activities, including excessive use of personal email, instant messaging, chat rooms, social media, etc.
- • Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- • Making unauthorized copies of company files or other company data;
- • Destroying, deleting, erasing, or concealing company files or other company data, or otherwise making such files or data unavailable or inaccessible to the company or to other authorized users of company systems;
- • Misrepresenting oneself or the company;
- • Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- • Engaging in unlawful or malicious activities;
- • Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the company's networks or systems or those of any other individual or entity;
- • Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- • Sending, receiving, or accessing pornographic materials;
- • Becoming involved in partisan politics;
- • Causing congestion, disruption, disablement, alteration, or impairment of company networks or systems;
- • Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;
- • Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- • Using recreational games;
- • Defeating or attempting to defeat security restrictions on company systems and applications.

Using company electronic systems or accounts to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the company anti-harassment policies and subjects the responsible employee to disciplinary action.

The company's electronic mail system, internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

SECTION F

No Expectation Of Privacy

The company owns the rights to all data and files in any computer, network, corporate account or other information system used in the company and to all data and files sent or received using any company system, account, cloud storage or using the company's access, including remote access, to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property.

The company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment or accounts used to create, view, or access e-mail and Internet content.

Employees must be aware that the electronic mail messages sent and received using company equipment corporate accounts, company-provided Internet access, and/or corporate accounts, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by company officials at all times. Only authorized personnel* have the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with company policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the IT Manager or OCE.

The company may use software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with company electronic systems or corporate accounts.

Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on company electronic systems or corporate accounts is electronically stored and subject to inspection, monitoring, evaluation, and company use at any time. Further, employees who use company electronic systems or corporate account to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure.

Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than company electronic systems or the corporate accounts. However, no company-related business should ever be sent or received via personal email or other communication accounts.

The company has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee

may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

SECTION G

Confidentiality Of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and company rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

SECTION H

Internet & Intranet

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

SECTION I

Authorized Personnel Defined

The following are authorized to access or to grant access to all systems as defined above:

- • IT Manager
- • Internal Tech Support
- • Contracted External Tech Support
- • Members of the OCE

SECTION J

Policy Violation

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

Violating any of these policies may result in disciplinary action, up to and including dismissal.