Laboratories at Adventist Healthcare Washington Adventist Hospital, Shady Grove Medical Center and Germantown Emergency Center

Date: November 22, 2016

LABORATORY ALERT

Subject: Computer and Network Use Policy

The Laboratory is informing you of the following

Information from AHC President & CEO:	Last week, Adventist HealthCare's computer system monitoring tools discovered a computer malware virus that required the Information Technology (IT) team to execute its Incident Response Process. This particular malware exhibited the most dangerous behavior that our security program protects against. In efforts to isolate the threat, AHC came very close to shutting down critical care IT services as a preventative measure to ensure our systems would not be compromised. The IT security team was able to address the situation before this action was required. **However, this step could have been avoided entirely as the event was caused by a staff member downloading and installing unapproved software for printing coupons.** As per our Computer and Network Use Policy (AHC 6.42), AHC employees are **not** to install any unauthorized or non-standard software. Installation of authorized software or equipment must be performed by IT. The policy applies to all employees, physicians, board members, contractors and volunteers who use electronic and computing devices; network resources to conduct business, clinical or patient care; or interact with internal networks and business systems, whether owned or leased by AHC, the employee, physicians, volunteers, board members or a third party. This policy contributes to ensuring our IT infrastructure and systems maintain functionality and support our clinical workflows. It is imperative that everyone adhere to this policy when conducting computer operations on the AHC computing platform.
Lab Staff expectations:	Carefully read and review the attached AHC policy by Dec 7, 2016. Always adhere to the AHC policy.
Contacts:	Laboratory management team
LBarrett/11.22.16	

G:\AHC_Lab\Clinical Folders\Communication_General Lab\Lab Alerts

ADVENTIST HEALTH CARE, INC.

CORPORATE PROCEDURE MANUAL

Computer and Network Use Policy

Effective Date:	02/09/16	**Policy No**:	AHC 6.42
Cross Referenced:		**Origin**:	IT
Reviewed:		**Authority**:	SET
Revised:		**Page**:	1 of 5

Purpose

AHC technology and devices are defined by Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, internet browsing, and any file sharing mechanism including FTP, SFTP, Cloud storage are the property of AHC. These systems are to be used for business purposes in serving the interests of the company, and of our clients and patients in the course of normal operations and patient care. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

This policy is to outline the acceptable use of technology and devices connecting to the network by all workforce members. These rules are in place to protect the workforce member and AHC. Inappropriate use exposes AHC and patients to risks including virus attacks, compromised network systems and services, and legal issues.

Scope

This policy applies to all workforce members who use electronic and computing devices, and network resources to conduct business, clinical or patient care or interact with internal networks and business systems, whether owned or leased by AHC, the employee, or a third party, physicians, volunteers, board members, and business associates (AHC Members).

Policy

General Use and Ownership

- You are responsible for reviewing, understanding, and adhering to AHC IT policy governing both technology and data usage.
- AHC's proprietary information stored on the network, the cloud, electronic and computing devices whether owned or leased by AHC, the employee or a third party, remains the sole property of AHC. You must ensure through legal or technical means that proprietary information is protected in accordance with AHC 6.30 Data Handling and Exchange policy.

- You are responsible for exercising good judgment regarding appropriate use of AHC resources in accordance with AHC policies, standards, and guidelines, as well as local, state, and Federal laws and regulations. AHC resources may not be used for any unlawful or prohibited purpose.

- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

- You may access, use or share proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

- For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time, per AHC's Internal Audit Policy.

- AHC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Devices that interfere with other devices or users on the AHC network may be disconnected. Information Security may block authorized audit scans if it interferes with normal traffic or business workflow. Firewalls and other blocking technologies must permit access to the scan sources.

System Accounts

- 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. Please refer to AHC 6.8 Access Control and AHC 6.8.1 Password Management Policy

- You must maintain system-level and user-level passwords in accordance with the Password Management Policy.

- You must ensure through legal or technical means that proprietary information remains within the control of AHC at all times. Conducting AHC business that results in the storage of proprietary information on personal or non-AHC controlled environments, including devices maintained by a third party with whom AHC does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by AHC, or its customer and partners, for company business. Gmail, Yahoo, Hotmail are examples.

Computing Assets

- You are responsible for ensuring the protection of assigned AHC assets that includes the use of computer cable locks and other security devices. Laptops left at AHC overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of AHC assets to your manager or the Service Desk.

- All mobile devices, PCs, laptops, and workstations, if technical feasible, must be secured with a password-protected screensaver or lock screen with the automatic activation feature set to 15 minutes or less, depending on your working environment. You must lock the screen or log off when the device is unattended.
- Devices that connect to the AHC network must comply with the Minimum Access Policy.
- Do not interfere with corporate device configuration management or security system software, including, but not limited to, antivirus, web filter, encryption or any other security software.
- Do not install any unauthorized or non-standard software. Installation of authorized software or equipment must be performed by IT.
- Non-IT staff is prohibited from moving non-mobile hardware. All staff must obtain approval based on work order or ticket to move any hardware.

Network Use

You are responsible for the security and appropriate use of AHC network resources under your control. The following activities are strictly prohibited:

- The use of devices to access production AHC networks for anything other than work purposes.
- The use of wireless connectivity for non-AHC devices on any wireless network other than the Physician_Guest and AHC guest network.
- Sharing of wireless keys and passwords by those individuals who have been issued the wireless key or password. Please also refer to AHC 6.41 Wireless Security Policy.
- Accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic. Please refer to AHC 6.1 Information System Security, Confidentiality & Password Assignment policy, AHC 6.30 Data Handling & Exchange policy, AHC 6.39 Remote Access and AHC 6.27 Public/Guest Access to IS resources.

- Introducing any non-AHC approved technology or software on the AHC network.

- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software. See the AHC 6.4 Software Licensing, Usage and Standards Policy for additional information on copyright restrictions.

- Use of the Internet or AHC network that violates AHC policies, or local laws. Please refer to AHC 6.5 Use of Electronic Mail & Internet Policy

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

- Port scanning or security scanning on a production network unless authorized in advance by Information Security, the Director of IT Infrastructure or the CIO.

Electronic Communications

The following are strictly prohibited:

- Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates AHC policies against harassment or the safeguarding of sensitive, confidential or proprietary information including Personally Identifiable Information (PII), Protected Health Information (PHI), Payment Card Industries (PCI) and Intellectual Properties.

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

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

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups using AHC email address.

- Use of AHC e-mail or IP address to engage in conduct that violates AHC policies or guidelines. Posting to a public newsgroup, bulletin board, social media or listserv with a

AHC e-mail or IP address represents AHC to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company. Please refer to AHC 6.32 Social Network Policy and AHC 6.5 Use of Electronic Mail (E-mail) & Internet policy.

Exceptions

Authorized personnel may be exempted from restriction mentioned above during their course of their legitimate job responsibilities. Any exception to this policy must follow a risk security assessment process and must be approved by the CIO in advance.

Non-Compliance

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please refer to AHC 2.0 Employee Conduct and AHC 2.76 Resignation and Termination policies.