ADVENTIST HEALTH CARE, INC.
CORPORATE POLICY MANUAL
Workstation Use & Security

Effective Date:	05/09	**Policy No**:	AHC 6.25
Cross Referenced:		**Origin**:	IT
Reviewed:		**Authority**:	EC
Revised:		**Page**:	1 of 7

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Adventist Healthcare (AHC). These rules are in place to protect both the employee as an individual and Adventist Healthcare as a company. Inappropriate use exposes Adventist Healthcare to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, vendors, physicians, volunteers, board members, and business associates (AHC Members). This policy applies to all equipment or systems that are owned or leased by AHC or PHNS Inc. for which PHNS Inc. has care, custody, or control on behalf of AHC. Additionally, this policy applies to all equipment or systems that connect to the AHC network or which stores AHC data.

Definitions

Mobile device: Any electric device that can be easily transported, and that has the capability of storing, processing and/or transmitting data, including but not limited to: laptops, tablets, mini hard drives, back-up hard drives, Zip Drives, Flash Drives, Personal Data Assistants (i.e. PDAs, including but not limited to Blackberries), Smart Phones, Hand Held/ pocket PCs, or any other mobile device designed or modified to store, process and/or transmit data.

Workstation: any electronic computing device, such as laptops, desktops, PDAs, smart phones, or any other device that performs similar functions or stores electronic media.

Employee: an AHC Member (see below).

General Information

AHC Members should be aware that the data they create on corporate systems remains the property of AHC. Employees should note that any data and information on the system will not be deemed personal or private. Employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, employees should consult their supervisor or manager. Examples of confidential information include but are not limited to: corporate strategies, competitor sensitive trade secrets, pricing terms and contracts, specifications, employee data, customer lists, research data and Protected Health Information

(PHI). Employees are required to take reasonable steps to prevent unauthorized access to this information.

***Monitoring**:* PHNS Inc., on behalf of AHC, provides and/or manages the network, workstations, electronic mail and other communications devices for AHC business purposes. AHC (and PHNS Inc. as authorized by AHC) may access and disclose all data or messages stored or sent over its electronic mail system as appropriate (e.g. for the purpose of routine maintenance, security, regulatory reporting, etc.). AHC and PHNS Inc. reserve the right to monitor communication and data at any time, with or without notice, to ensure that company property is being used appropriately.

***Retrieval**:* Notwithstanding the company's right to retrieve and read any electronic data or information, i.e. e-mail messages, such data must be treated as confidential by all employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any electronic data that is not sent to them and cannot use another's identity or password, access a file, or retrieve any stored information, unless authorized to do so.

***Legal Proceedings**:* Information sent by employees via the electronic mail system may be used in legal proceedings. Electronic mail messages are considered written communications and may be subject to subpoena in litigation. AHC (and PHNS Inc. as authorized by AHC) may inspect the contents of electronic mail messages in the course of an investigation, will respond to the legal process, and will fulfill any legal obligations to third parties.

Policy

1. Acceptable Use

***Passwords**:* Initial passwords are assigned by the system administrator. Employees are required to change the provided passwords as soon as possible, but no longer than one business day, to the extent the systems allows using strong password criteria (8 character minimum, including: 1 upper case, 1 lower case, 1 number, 1 special character). PHNS Inc. reserves the right to override any employee-selected passwords and/or codes to facilitate access as needed to carry out the business of AHC or PHNS Inc. Periodically, staff may be required to change their passwords. Passwords may **not** be shared and if written down must be stored in a secure location. Passwords should never be affixed in plain view on or near the workstation, and users may not save fixed passwords in web browsers or e-mail clients when using a PHNS system.

***Software**:* Only legally licensed software will be installed on AHC or PHNS Inc. workstations; software cannot be purchased, installed, or copied without the permission or involvement of PHNS Inc. Staff members are not permitted to download or install applications, demos or

upgrades. PHNS Inc. will configure all workstations with virus protection software, which may not be removed or disabled. All data disks and files entering AHC must be scanned for viruses. In addition to virus software, each employee is responsible for protecting their computer against virus attacks (such as scanning files after they have been downloaded but before they are opened). Personal email accounts should not be used for transferring/downloading software or data.

When leaving a workstation unattended during their shift, the device must be logged off or locked or configured to use an automatic password protected screen savers. All staff will shut down, log off or lock the workstation at the end of their shift, and are required to restart their workstations twice a week to allow updates to install.

Data stored on the local PC drive (i.e., C:) is not routinely backed up. Therefore, important data must be placed on the respective network drive (i.e., F:, G:) to guarantee the information is backed up. Network drives may not be used to store or backup non-business documents or data files.

***Internet Use**:* The Internet is to be used for business purposes only, minor, non-commercial, personal use may be permitted at management's discretion. Internet usage is monitored. Employees with Internet access are expressly prohibited from accessing, viewing, downloading, or printing pornographic or other sexually explicit or offensive materials. Company information or business may not be sent unless using company provided internet based tools, including e-mail and/or instant messaging.

If the employee leaves the organization, he or she must return all workstation(s) and related equipment (i.e. Laptops, zip/jump/flash drives, printers, modems etc.) to AHC by the last day of employment. All business related data will not be deleted prior to returning the equipment.

2. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., an AHC Manager may need to access an employee's email account while they are out on long-term leave).
Under no circumstances is an employee of AHC authorized to engage in any activity that is illegal under local, state, or federal laws or regulations while utilizing AHC or PHNS Inc.-owned resources.

The list below is by no means exhaustive, but is intended to provide a framework for activities which fall into the category of unacceptable use.

a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PHNS Inc. or AHC.
b. Introduction of malicious programs onto the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
c. Revealing your account password to others or allowing use of your account by others.
d. Using an AHC or PHNS Inc. computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
e. Making fraudulent offers of products, items, or services originating from any AHC or PHNS Inc. account.
f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to port scanning or security scanning, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
g. Circumventing user authentication or security of any host, network or account.
h. Providing AHC or PHNS Inc. proprietary information to unauthorized parties.
i. Disabling of the antivirus client.
j. Using the e-mail system to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. The e-mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
k. The e-mail system may not be used to send (upload) or receive (download) non-public copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
l. Removal of an asset tag from equipment.
m. Installing P2P File sharing software on any AHC workstation or mobile device.

3. Workstation Management

Add: When a new workstation is brought into an area or department the department manager or designee will need to sign a form acknowledging receipt of the workstation.

Move: Anytime a device is moved within the department (re-assigned to another individual) PHNS must be notified via the service desk (user will be required to provide device ID).

Change: In the event a workstation needs to be replaced, the department manager or designee will be required to sign an acknowledgment of the removal of one workstation and the receipt of a new workstation.

Remove: Any time a mobile device is no longer needed or is pending re-assignment (e.g. an employee leaves and the new hire has not been found) the device must be returned to PHNS.

All documentation regarding add, move, change, or remove must include the asset tag number, facility, department, physical location, management signature, and date.

Management will be required to conduct a quarterly validation of IT inventory.

4. Mobile Devices

Mobile device users are responsible for protecting the information processed, stored, or transmitted over or on mobile resources and are responsible for securing their devices and other forms of portable media at all times.

All AHC laptop computers shall be setup to automatically encrypt designated data contained on them according to established security policies regardless of the current or future presence of PHI.

AHC mobile devices actively connected to the network or information systems **and** not on the premises must not be left unsecured.

When in transit AHC mobile devices shall be secured to prevent theft. If the device is left unattended in the vehicle, it must be placed in the trunk, under the vehicle's seat out of sight, or taken with you. AHC mobile computers shall never be left unattended while located in facilities other than AHC facilities (i.e. vendor’s offices, customer sites) unless the work space has been physically secured.

Individual, AHC mobile devices and/or IT resources shall not be stored in checked luggage while traveling, whether it is an international or a domestic flight. Multiple computers being used for training or demonstrations may be sent in a secure container as checked luggage. If the mobile device cannot be carried on board, an alternate means of transportation shall be found for the device. AHC mobile device users shall ensure a direct line of sight to minimize the potential for damage or theft while passing through security checkpoints (e.g., airports and train stations). Employees carrying AHC issued laptops or other electronic data mobile devices while traveling

abroad, whether on business or for pleasure, must comply with U.S. trade control laws and receive documented approval from the ACH Chief Privacy & Security Officer before a mobile device is taken overseas.

When a laptop requires a hardware upgrade (e.g., memory, peripheral, or hard disk), software installation, or has problems that cannot be resolved over the telephone, a POB case must be opened and the computer may need to be brought to a designated site for hardware service, software installation, or problem diagnosis.

PDAs, Smart Phones, and other hand held devices are not considered a secure computing device. It is required that only non-confidential information be stored on the device and the password protection feature is enabled. PDAs are supported in the following ways:

a. Full Support: provided on all hand held computers purchased and owned by AHC, includes: purchase of equipment, repairs and replacements. GroupWise address book synchronization. GroupWise calendar synchronization, GroupWise e-mail synchronization, GroupWise Task synchronization.
b. Limited Support: hand held computers owned by users and that are **not** synced at home will have limited support, including: GroupWise addresses book synchronization, GroupWise calendar synchronization, GroupWise e-mail synchronization, GroupWise Task synchronization. Desktop Services is not responsible for hardware repairs or replacements.
c. Not Supported: hand held computers that are not AHC owned and that are synced at home are not supported

5. Reporting

Users are responsible to immediately report any incidents involving mishandling, tampering with, or losing a workstation or mobile device that contains company or confidential data to their, Entity Chief Privacy & Security Officer, the AHC Chief Privacy & Security Officer, the Director of Corporate Security, and the PHNS Compliance Specialist. Do not discuss information security-related incidents with individuals outside of AHC or PHNS, or with those inside AHC or PHNS who do not have a need-to-know. (Reference: Incident Handling Policy and Data Handling/Transmission Policy).

6. Compliance

Failure to comply with any component of the Workstation Use & Security Policy may result in disciplinary action up to and including termination of employment. If the AHC member does not

understand any part of the policy, it is their responsibility to obtain clarification from their manager or PHNS Inc.

Reference:

A. AHC 4.5 HIPAA Privacy
B. AHC 6.1.1 Computer Security Agreement
C. AHC 6.4.1 Software Code of Ethics