DEPARTMENT: HUMAN RESOURCES	POLICY DESCRIPTION: COMMUNICATIONS SYSTEM - ACCEPTABLE USE
APPROVED:	REVIEWED:
REPLACES: POLICY DATED 06/99, COMMUNICATION SYSTEMS DATED 09-01-04, AND ACCEPTABLE USE POLICY CREATED ON 03/27/2012	RETIRED:
ADOPTED:	REVISED: 12/12/2016
Page 1 of 10	REFERENCE NUMBER: C-VI-13

SCOPE: All full-time and part time employees of ARH and business partners.

PURPOSE: Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

DEFINITIONS: Appalachian Regional Healthcare is hereinafter referred to as "the company."

Blogging The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

PROCEDURE:

I. E-mail Use

Personal usage of company email systems is prohibited. Users should use corporate email systems for business communications only.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.

- The user is prohibited from forging email header information or attempting to impersonate another person.

- Email is an insecure method of communication, and thus PHI may not be sent via email, outside of ARH without proper encryption.

- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of 5mb or larger.

Please note that detailed information about the use of email may be covered in the company's Email Policy.

II. Confidentiality

Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

III. Network Access

The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this

access.

IV. Unacceptable Use

The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

V. Blogging and Social Networking

Blogging and social networking by the company's employees are subject

to the terms of the *Social Media and Social Networking Policy, C-IV-25*, whether performed from the corporate network or from personal systems. Blogging and social networking is only allowed from the corporate computer network when it is approved company business. In no blog or website, including blogs or sites published from personal or public systems, shall the company business matters discussed, or material detrimental to the company published. The user assumes all risks associated with blogging and/or social networking.

VI. Instant Messaging

Instant Messaging is allowed only on approved cases. The user should recognize that Instant Messaging may be an insecure medium and should take any necessary steps to follow guidelines on disclosure of confidential data.

VII. Overuse

Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.

VIII. Web Browsing

The Internet is a network of interconnected computers of which the company has very little control. The user should recognize this when using the Internet, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. The company is specifically not responsible for any information that the user view, reads, or downloads from the internet.

Intentionally attempting to browse or download material that is deemed inappropriate, sexually explicit or profane is expressly prohibited.

Personal use of company computer systems to access the Internet is not permitted under any circumstances.

IX. Copyright Infringement

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized

copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

X. Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.

XI. Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

XII. Monitoring and Privacy

Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

XIII. Bandwidth Usage

Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.

XIV. Personal Usage

Personal use of company computer systems is not permitted under any circumstances.

XV. Remote Desktop Access

Use of remote desktop software and/or services is allowable as long as it is provided by the company. Remote access to the network must conform to the company's Remote Access Policy.

XVI. Circumvention of Security

Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

XVII. Use for Illegal Activities

No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identify Theft

- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
- Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.

XVIII. Non-Company-Owned Equipment

Non-company-provided equipment is expressly prohibited on the company's network.

XIX. Personal Storage Media

Personal storage devices represent a serious threat to data security and are expressly prohibited on the company's network unless explicitly approved by IT manager.

XX. Software Installation

Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.

XXI. Reporting of Security Incident

If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information

- Loss or theft of ID badge or keycard
- Any attempt by any person to obtain a user's password over the telephone or by e-mail.
- Any other suspicious event that may impact the company's information security.

Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

XXII. Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

XXIII. Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

APPALACHIAN REGIONAL HEALTHCARE, INC.
STATEMENT OF USAGE, CONFIDENTIALITY, and SECURITY

A. The proper use of communication resources and information services at Appalachian Regional Healthcare, Inc. (ARH) applies to all employees, staff, vendors, and partners who access and utilize communication and information technology provided by ARH. All ARH communication and information resources (including but not limited to system, telephone, cellular phones, fax, electronic mail, voice mail, Internet, video-conferencing) however transmitted, accessed, or stored are the property of ARH. The information and data transmitted through these systems are confidential and proprietary to ARH. Only authorized users may access these systems. ARH may deny access to these services and reserves the right to inspect, monitor, or disclose any files or records.

B. Confidential information is valuable and sensitive and is protected by law and by strict ARH policies. The intent of these laws and policies is to assure that confidential information will be used only as necessary to accomplish the organization's mission. You are required to conduct yourself in strict conformance to applicable laws and ARH policies governing confidential information which may include, but is not limited to, information relating to:

- Patients/customers (such as records, conversations, admittance information, patient/member financial information, etc.)
- Employees/volunteer/students (such as salaries, employment records, disciplinary actions, etc.)
- ARH information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.)
- Third party information (such as computer programs, client and vendor proprietary information, source code, proprietary technology, etc.).

C. As a condition of use of ARH provided resources and services and in consideration of my access to confidential information,

I accept the following responsibilities and terms:

- Respect the intended use of all ARH provided communication and information resources. Limited personal use must not interfere with assigned duties and reimbursement must be made to ARH for any expenses that may result from personal use.
- Respect the procedures established to manage the use of the system.
- Respect the capability of the systems, and limit your own use so as not to interfere unreasonably with the activity of other users.
- Respect the ownership of proprietary and copyrighted software.
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my work assignment.
- Not operate any non-licensed software on any computer provided by ARH
- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment. Information accessed through all ARH systems should only be disclosed to those authorized to receive it.
- Not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.
- Not remove any original or copied record, file, or report from the office where it is kept except in the performance of my duties.
- Not release my identification code or password to anyone else, or allow anyone else to access or alter information under my identity.
- Accept responsibility for all activities undertaken using my identification code or password.
- Take appropriate action to change or request a change to my identification code or password if the confidentiality has been threatened.
- Not utilize anyone else's identification code, password, or other assigned authorization in order to access any ARH system.
- Respect the confidentiality of any reports printed from any information system and handle, store and dispose of these reports appropriately.
- Access and utilize confidential information only for which you have a need to know.
- Report activities by any individual or entity that may compromise the confidentiality of information or violate other terms of this agreement.

D. I have read, understand, and agree to comply with the terms outlined in “Use of Communication and Information Resources, Technology and Networks at Appalachian Regional Healthcare, Inc”.

E. My signature below indicates that I have read, understand, and agree to comply with the terms outlined above. I understand the implications associated with disregard for any or all of the above requirements in regards to use of communication and information technology resources available at ARH and that the violation of any part of this agreement will subject vendor to discipline, which might include, but is not limited to, termination of services and/or legal liability. Those who cannot accept these standards of behavior may be denied access to the communication and information technology resources provided by ARH.

Signature:_____ Date:_____

Witness:_____ Date: _____

APPALACHIAN REGIONAL HEALTHCARE, INC.
AFFILIATED USER AND STUDENT
STATEMENT OF USAGE, CONFIDENTIALITY, and SECURITY

A. The proper use of communication resources and information services at Appalachian Regional Healthcare, Inc. (ARH) is required of all employees, staff, vendors, students, and partners who access sensitive information and who otherwise utilize communication and information technologies provided by ARH. All ARH communication and information resources (including, but not limited to any and all information transmitted, received, stored or accessed from telephones, whether base or cellular, fax, electronic mail, voice mail, internet, video-conferencing), however transmitted, accessed, or stored, are the property of ARH. The information and data transmitted through these systems are confidential and proprietary to ARH. Only authorized users may access these systems. ARH may deny access to these services at its sole discretion, and reserves the right to inspect, monitor, or disclose any files or records generated by any of its information systems.

B. Confidential information is valuable and sensitive, and is protected by law and by ARH policies. The intent of these laws and policies is to assure that confidential information will be used only as necessary to accomplish the ARH mission. You are required to conduct yourself in strict compliance with applicable laws and ARH policies governing confidential information which may include, but is not limited to:

- Patients/customers (such as records, conversations, admittance information, patient/member financial information, etc.)
- Employees/volunteer/students (such as salaries, employment records, disciplinary actions, etc.)
- ARH information (such as financial and statistical records, strategic plans, internal reports, memos, contracts, peer review information, communications, proprietary computer programs, source code, proprietary technology, etc.)
- Third party information (such as computer programs, client and vendor proprietary information, source code, proprietary technology, etc.).

C. As a condition of use of ARH provided resources and services, and in consideration of ARH's express permission granting my access to confidential information,

I hereby accept the following obligations and responsibilities:

- Respect the intended use of all ARH provided communication and information resources. Limited personal use must not interfere with assigned duties, and reimbursement must be made to ARH for any expenses that may result from personal use.
- Respect the procedures established to manage the use of the system.
- Respect the capability of the systems, and limit your own use so as not to interfere unreasonably with the activity of other users.
- Respect the ownership of proprietary and copyrighted software.
- Avoid activities related to personal benefit, or permit others to benefit personally by any use or disclosure of confidential information or use of equipment available through my work assignment.
- Avoid use of any non-licensed software on any computer provided by ARH
- Do not exhibit or divulge the contents of any record or report except to fulfill a work assignment. Information accessed through all ARH systems should only be disclosed to those authorized to receive it.
- Do not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.
- Do not remove any original or copied record, file, or report from the office where it is kept except in the performance of my duties.
- Do not release my identification code or password to anyone else, or allow anyone else to access or alter information under my identity.
- Accept responsibility for all activities undertaken using my identification code or password.
- Take appropriate action to change or request a change to my identification code or password if the security or confidentiality thereof has been compromised or potentially threatened.
- Do not utilize anyone else's identification code, password, or other assigned authorization in order to access any ARH system.
- Respect the confidentiality of any reports printed from any information system and handle, store and dispose of these reports appropriately.
- Access and utilize confidential information *only* for which you have a need to know.
- Report activities by any individual or entity that may compromise the confidentiality of information or violate other terms of this agreement.

D. My signature below indicates that I have read, understand, and agree to comply with the terms outlined above. I understand the responsibilities associated with disregard for any or all of the above requirements in regards to use of communication and information technology resources available at ARH, and that the violation of any part of this agreement will subject the user to discipline, which might include, but is not limited to, termination of services and/or legal liability, and denial of further access to the communication and information technology resources provided by ARH.

Signature: _____ Date: _____

Witness: _____ Date: _____