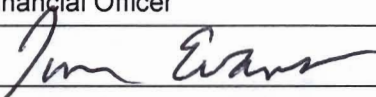
	SECTION: Administrative Manual	Page 1 of 5
	NUMBER: QSP-ADM-MI-0004	Revision Level: 4
FORMULATED: 2/05	TITLE: IT Acceptable Use Policy	
REVISED: 8/05, 7/11, 8/14, 9/16	APPROVAL: Tim Evans TITLE: Chief Financial Officer	
REVIEWED: 6/10/13, 8/27/14, 5/23/16	SIGNATURE: 	
<p>This document contains information of a proprietary nature. Information contained herein shall be kept in confidence and divulged only to persons who by nature of their duties require access to such documentation.</p>		

Policy Statement:

Self Regional Healthcare and its subsidiaries (“SRH” or the “Organization”) rely heavily on computer resources to conduct business. As such, this policy is designed to provide specific guidelines for “Users” (as defined below) concerning the use of all forms of electronic media and services provided by the Organization to ensure that such use is consistent with the legitimate business interests of the Organization.

With the rapidly changing nature of electronic media and services, this Acceptable Use Policy cannot establish rules to cover every possible situation. Instead, it expresses the Organization’s philosophy and sets forth principles to be applied to the use of all electronic media and services now in existence or which may be utilized by the Organization in the future.

Scope / Responsibility:

The term, “Users,” shall include, but is not limited to, SRH team members and persons who are not employed by SRH, but who are accessing or developing Self Regional Healthcare’s Electronic Media and Services, directly or indirectly, including but not limited to, engineers, contractors, consultants, vendors and temporary workers. All Users of SRH Electronic Media and Services are required to sign this Acceptable Use Policy before accessing any SRH Electronic Media and Services.

The forms of electronic media and services governed by this policy include desktop computers, laptop computers, peripherals, e-mail, wireless and IP based handheld devices, pagers, desk phones, wireless phones, cellular phones, smart phones, on-line services, the Internet, Extranet, FTP sites, software, data file access, applications, and any other information systemic media or services which may be developed and/or utilized by the Organization in the future (hereinafter collectively referred to as “Electronic Media and Services”).

This policy applies to all Users who access any non public Electronic Media or Services from any SRH owned equipment or non-owned equipment while residing on or accessing through the SRH network:

- a. On or off SRH premises;
- b. Using SRH equipment or resources;
- c. Via SRH-paid access methods; such as remote access and Internet connections
- d. Users who use any Electronic Media or Services in a manner which identifies the User with SRH and/or which references SRH in any manner.

This policy does not apply to all Users who access any Electronic Media and Services that are offered to the general public (e.g. www.selfregional.org, public FTP servers).

Process:

1. SRH owned computer resources are the Organization’s property. All Electronic Media and Services used or developed by Users while employed or contracted at SRH are the property of Self Regional Healthcare.
2. Users should have no expectation of privacy. Please refer to the Information Security Monitoring Procedure for specific guidelines on the process of monitoring Information Technology systems and/or data.
3. Users using e-mail and other forms of electronic communications should exercise the same care and professional demeanor in those communications as used in writing letters, memos and other paper messages. E-mail and other forms of electronic communications may be preserved or may be recoverable long after they are deleted.

FORMULATED: 2/05

TITLE: IT Acceptable Use Policy

REVISED: 8/05, 7/11, 8/14, 9/16

APPROVAL: Tim Evans
TITLE: Chief Financial Officer

REVIEWED: 6/10/13, 8/27/14, 5/23/16

SIGNATURE: 

4. Personal use of Electronic Media and Services will be monitored according to the standards set in the Information Security Monitoring Procedure. Electronic Media and Services covered under this Acceptable Use Policy are to be used for SRH-related business purposes. They may not be used for the purpose of conducting personal business, for personal gain or for furthering a User's political, religious or other personal causes. Reasonableness and common sense are the guiding principles. Supervisors and managers will determine whether SRH Electronic Media and Services are being used for excessive personal use by a User. Supervisors or managers should contact their administrator when made aware of any misuse or security incidents.
5. Recreational Internet "Surfing" for non-business related activities is prohibited. Users shall not use the Organization's Internet connection for visiting or downloading information from non-business-related Web sites. Specific examples of non-business-related Web Sites include but are not limited to, those which contain discriminatory or harassing materials, pornography, nudity or foul language. Any access to external on-line services through the Internet is limited to only those Internet sites which have relevance to the User's work with Self Regional Healthcare. Reasonableness and common sense are the guiding principles based on but are not limited to the following standards.
 - a. Access, retrieve, or print text and graphics information which exceeds the bounds of generally accepted standards of good taste and ethics.
 - b. Engage in any unlawful activities or any other activities which would in any way bring discredit on the Organization.
 - c. Engage in personal commercial activities on the Internet, including offering services or merchandise for sale or ordering services.
 - d. Engage in any activity which would compromise the security of any SRH host computer.
 - e. Engage in any activity not endorsed by the Organization. Such activities include but are not limited to: fund raising, endorse any product or services, participate in any lobbying activity, or engage in any active political activity.
6. Use of another user's User-Id or password is prohibited. The Organization issues User Identifiers ("User Ids") and users of the Electronic Media and Services create passwords as tools to help ensure data security. Users are responsible for safeguarding their User Ids and passwords. Additionally, except as set forth above, all messages sent via e-mail are considered confidential and as such are not to be read, altered or copied by anyone other than the addressed recipient(s), unless specific authorization to do so is given as defined in the Information Security Monitoring Procedure.
7. Users must respect the confidentiality of SRH computer systems and the computer systems of individuals and firms not affiliated with the Organization. Users may not attempt on SRH or third party systems the following malicious activities:
 - a. "Hack" into the computer systems
 - b. Breach computer or network security measures
 - c. Monitor electronic files or communications of SRH or third parties.
8. Precautions to Avoid Virus and other Data Security Breaches Must Be Taken. Each User using the Electronic Media and Services provided by the Organization is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the SRH computer network. To that end, all material received on CD, DVD, thumb/jump drive or other magnetic/optical medium and all material downloaded from the Internet or from other sites not a part of the Self Regional Healthcare network system must be scanned for viruses. Remote Users accessing the Internet through a computer attached to the Self Regional Healthcare network must do so through an approved Internet firewall or one provided by SRH on a permanent or temporary basis. Accessing the Internet directly by modem is strictly prohibited unless the

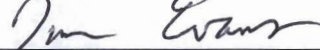
FORMULATED: 2/05

TITLE: IT Acceptable Use Policy

REVISED: 8/05, 7/11, 8/14, 9/16

APPROVAL: Tim Evans
TITLE: Chief Financial Officer

REVIEWED: 6/10/13, 8/27/14, 5/23/16

SIGNATURE: 

computer being used has access to a secure Virtual Private Network (VPN), Citrix remote access, and/or is not connecting to the Organization's network.

9. Neither non-SRH computer systems nor any type of non-SRH owned networkability device shall be used to access or "plug in to" SRH production networks or other SRH Electronic Media and Services without specific prior approval from Self Regional Healthcare. Non-owned equipment needing access to such services as the Internet will be granted "Guest" access and be monitored by the same standards set forth in this policy for Users of SRH owned equipment. Users of non-owned equipment must also take the same precautions as Users utilizing SRH owned equipment for preventing the spread of computer viruses into the SRH network.
10. Intellectual property rights of others must be respected. Each User shall respect the intellectual property rights of others when utilizing Electronic Media and Services. Prior to any information on the Internet being copied or downloaded to a personal computer provided by the Organization, it is the responsibility of the User accessing the information to ensure that it is free of any copyright restrictions. Any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law and, thus, is specifically prohibited.
11. All software and hardware as it is related to Information Systems & Technology shall be purchased and installed by the Information Systems & Technology Department. All software and hardware used by Users to perform their job functions shall be purchased and installed by the Information Systems/Technology Department. No unapproved software is to be loaded on Self Regional Healthcare equipment. Requests for new software or hardware and its installation must be approved by a department manager or head and then approved by the Director of Information Systems & Technology and Chief Financial Officer for budget procurement recommendation.
12. Illegal, inappropriate and harassing communications are prohibited. Users are prohibited from using Electronic Media and Services to transmit, retrieve or store any communication, which is either:
 - a. Discriminatory or harassing in nature;
 - b. Derogatory to any individual or group;
 - c. Defamatory or threatening; or
 - d. Contrary to the legitimate business interests of the Organization
13. Waste of computer resources is prohibited. Users may not use Electronic Media and Services in a manner that wastes SRH computer resources or is likely to cause network congestion or significantly hamper the ability of other Users to access and use the system. Uses that may congest the Electronic Media and Services include, but are not limited to, sending mass mailings or chain letters, sending large documents or attachments through the email system, streaming video, and spending excessive amounts of time on the Internet.
14. Confidentiality and integrity of information shall be protected. In using Electronic Media and Services, Users will have access to Self Regional Healthcare's regulated, proprietary, and other confidential information. Protection of this information and the equipment used to view it plays a vital role in the Organization's continued growth and ability to meet compliancy. In addition, Users should not disclose this information to other Users except where appropriate based on business need, accompanied by a written statement, where feasible, that the information is confidential and being provided for the purpose of permitting a User to perform the duties of his or her job with the Organization properly. The transmission of SRH confidential information, which includes but is not limited to: SRH proprietary information, SRH financial information, and Electronic Protected Health Information, must be encrypted and based on business need.
15. It is the intention of this policy that in addition to current email security practices and where appropriate, digital certificates and/or encryption may be utilized to protect information being transmitted via the SRH E-Mail system. Furthermore all users of the SRH E-Mail system should attach the following banner as a standard signature for all E-Mails sent within and outside the Organization.


FORMULATED: 2/05

TITLE: IT Acceptable Use Policy

REVISED: 8/05, 7/11, 8/14, 9/16

APPROVAL: Tim Evans
TITLE: Chief Financial Officer

REVIEWED: 6/10/13, 8/27/14, 5/23/16

SIGNATURE: 

"This electronic message transmission, including any attachments, contains information from Self Regional Healthcare which may be confidential or privileged. The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of the communication, including attachments."

16. Misuse must be reported. Users learning of any misuse of the Electronic Media or Services are expected to report such misuse to their immediate supervisor or department head. Supervisors and department heads should in turn contact the administrator for their area when made aware of any misuse or security incidents. Anonymous reporting of misuse as per the SRH Corporate Compliance policy is also a proper means of communicating misuse within the organization.
17. Social media is defined by this policy as any online tool that people use to share content, profiles, opinions, insights, experiences, perspectives and media, thereby facilitating conversations and interaction online between individuals as well as groups of people. These tools include blogs, message boards, podcasts, micro blogs, livestreams, bookmarks, networks, communities, wikis, and vlogs. Example of social media include Facebook, Twitter, LinkedIn, YouTube, etc.
18. Access to social media resources from the SRH network will be granted for business purposes only. Requests for access to social media resources must be submitted via the Security Request Form and will be processed through the Security Request Process.
19. Users should have no expectation of privacy when accessing social media from the SRH network. Please refer to the Information Security Monitoring Procedure for specific guidelines on the process of monitoring Information Technology systems and/or data.
20. Users must not post confidential information. Confidential information includes, but is not limited to, SRH proprietary information, SRH financial information, and Electronic Protected Health Information (ePHI).
21. Users must adhere to the Code of Ethics / Self Standards at all times while utilizing social media services
22. Users representing SRH in a social media setting must disclose their relationship with SRH and all communications should be consistent with SRH values, policies and applicable laws.
23. Team Members, physicians, volunteers or other associates of SRH not acting in an official capacity should include a disclaimer in their online communications advising that they are speaking personally and not on behalf of the organization. Individuals may be held personally liable for defamatory, proprietary or libelous commentary.
24. Any questions concerning the application of this Acceptable Use Policy should be addressed to the User's immediate manager. Further clarification or interpretation of issues related to this policy should be forwarded to the administrator for their area.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action or legal action, up to and including termination of employment as defined in the SRH Sanction Policy.

References (if not noted elsewhere in policy):

n/a

Definitions:

n/a

FORMULATED: 2/05

TITLE: IT Acceptable Use Policy

REVISED: 8/05, 7/11, 8/14, 9/16

APPROVAL: Tim Evans
TITLE: Chief Financial Officer

REVIEWED: 6/10/13, 8/27/14, 5/23/16

SIGNATURE: 

Declaration

By signing this Acknowledgement Form below, I am indicating I have received the Acceptable Use Policy, dated _____, 20___, and I have read, understand and agree to abide by the policy.

Name (Signature)

Employee Number

Name (Print)

Position and Department

Date