Scripps

TITLE: Computer, Network, and E-mail Usage (Acceptable Use)
IDENTIFIER: S-FW-IM-2001

APPROVED: Executive Cabinet 05/07/13	**EFFECTIVE DATE**		
	☒ Acute Care	**ENC 05/13/13**	**GH 05/13/13**
ORIGINAL: 11/00		**LJ 05/13/13**	**MER 05/13/13**
	☒ Home Health	**05/13/13**	
REVISED: 03/03, 03/05, 07/07, 01/12, 05/13	**☒ Hospice**	**05/13/13**	
	☒ SMF	**05/13/13**	
REVIEWED:	**☒ SHAS**	**05/13/13**	

I. PURPOSE

The purpose of this policy is to outline the acceptable use of Scripps computer resources. These rules are in place to protect the users and other individuals granted access privileges and Scripps at Scripps comply with a multitude of applicable policies. Effective information security is a team effort involving the participation and support of every Scripps employee and third party who deals with information and/or information systems. It is the responsibility of every computer user to know the expectations per this policy and conduct their activities accordingly when accessing Scripps systems on premises and remotely.

The intentions for publishing this Acceptable Use Policy are not to impose restrictions that are contrary to Scripps established culture of openness, trust, and integrity. Scripps is committed to protecting the organization's users, physicians, and other third party partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

II. POLICY

A. Internet, e-mail, network, and application system access is granted to individuals for the purpose of supporting Scripps clinical and business activities necessary to carry out job functions and assigned duties.

B. **Acceptable Use and Ownership**

1. While Scripps desires to provide a reasonable level of privacy, system users must be aware that data they create on Scripps systems remains the property of Scripps. Therefore, Scripps system users must have no expectation of privacy for activities carried out on Scripps and non-Scripps computers.
2. The fact that an individual has the ability to access Confidential Information does not authorize that individual to access or use such information unless his or her job duties specifically require him or her to do so.
3. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Using Scripps computing resources for personal purposes, except in an incidental manner, may be considered cause for corrective action, up to and including termination. If there is any uncertainty as to expectations or your job duties as they relate to the use of computing resources, consult your supervisor or manager.
4. For security and network maintenance purposes, or to ensure compliance with this policy, authorized individuals within Scripps may monitor and audit

equipment, application systems and network traffic at any time and review logs in accordance with protocols established per Scripps Information Security Program Policy, S-FW-IM-3000.

5. Scripps management provides computer equipment, removable storage or mobile devices to employees and certain other users for accessing Scripps information systems for conducting Scripps business based on the user's job responsibilities. Scripps-issued computer equipment, removable storage or mobile devices should be used to connect to the Scripps network, systems and applications. In situations when Scripps-issued assets cannot be used to directly connect to the Scripps wired or wireless network, users are responsible for ensuring that Scripps confidential data is not stored, except by using Scripps-approved encryption mechanisms. Connecting a personal device in an unauthorized manner is considered a violation of this policy. When personal devices or computers are used to connect to Scripps information systems, network and application systems to conduct Scripps business, the user will be required to acknowledge their responsibility for complying with Scripps security recommendations on configuring the devices (software, passwords, encryption etc.) and will also be required to sign a 'consent to fully cooperate' with an investigation in the event that their personal device is reasonably suspected to have been compromised or involved in a security or privacy event. Should the user refuse to cooperate with any investigation deemed necessary, their privileges to connect to the Scripps network with a personal device may be suspended or revoked.
6. In the event of a suspected security or privacy event, the owner of any personal device suspected of containing Scripps confidential information understands that Scripps may take a digital forensic image of their personal device for review without making any changes to the data or software installed on the personal device. In these situations a *Scripps Personal Computer System Release of Liability Waiver* needs to be signed.
7. When using Scripps e-mail resources, accessing the Internet from their Scripps network Scripps login, or blogging while stating an affiliation with Scripps, users must recognize that they represent Scripps and must follow Scripps policies and be attentive to social media use guidelines.

C. **Safeguarding Confidential Information**

1. Keep passwords secure and do not share Scripps logins. Authorized users are responsible for the security of their passwords and Scripps logins.
2. All Scripps-owned desktop computers, laptops, handheld devices, and workstations used to conduct Scripps business must be secured with a password-protected screensaver with the automatic activation features set per Scripps current policy or by locking or logging-off when the computer/device is unattended.
3. Confidential data leaving Scripps must be protected through encryption or equivalent authorized mechanisms both while in transit and at rest.
4. Use encryption of information and other safeguards in compliance with Scripps Confidentiality of Information policy, S-FW-IM-0201.
5. Personal postings must be done using a personal e-mail login (not Scripps e-mail or Scripps login). Refer to Social Media Guidelines as part of the

Confidentiality of Information (Patient, Financial, Employee and Other Sensitive and Proprietary Information), S-FW-IM-0201.

6. To access Scripps network remotely, users must use the Scripps standard remote access solution and must use computers with updated anti-virus software and patches. Use of any other unauthorized remote access (such as PC Anywhere, GoToMyPC, LogMeIn, SSH, etc.) is prohibited.
7. Users must use caution when opening e-mail attachments or when clicking on hyperlinks received from unknown senders, as these e-mails may contain viruses, e-mail bombs, or Trojan horse code which can harm the Scripps network or clinical and business computing resources.

D. **Unacceptable Use**

Under no circumstances is a Scripps user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Scripps-owned resources.

The following activities are PROHIBITED:

Specific users may be exempted from certain of these prohibited activities during the course of their legitimate job responsibilities (e.g., systems administration staff carrying out their daily job duties asked to disable the network access of a computer/device if that computer/device is disrupting production services). The list below is not intended to be all inclusive, but attempts to provide a framework/guidance for identified activities which fall into the category of unacceptable use.

1. **System and Network Activities**

The following activities are strictly prohibited, with no exceptions.

a. Accessing, modifying or updating information that is not within the scope of your job duties (e.g. accessing patient information, including your own, for other than job-related reasons.) Accessing, downloading, or removing confidential information (encrypted or unencrypted) from Scripps without authorization from your supervisor and the Data Owner or specific job duty requirements. See Confidentiality of Information (Patient, Financial, Employee and Other Sensitive and Proprietary Information), S-FW-IM-0201.

b. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

c. Revealing your Scripps login session password to others or allowing others to use your Scripps login and password. This includes family and other household members when work is done at home.

d. Attempting to gain access to another's password or information or using someone's already logged-on session.

e. 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 Scripps.

f. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Scripps or the end user does not have an active license is strictly prohibited.

g. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate management must be consulted prior to export of any material that is in question.

h. Using a Scripps computer/device to view, acquire, store, or disseminate data that is illegal, pornographic, or in non-compliance with the Scripps Harassment-Free Workplace policy, S-FW-HR-0510.

i. Breaching security or causing intentional disruptions to network communication (see Attachment A: Glossary for examples of Security Breaches).

j. Providing information about, or lists of, Scripps users to third parties without authorization by your supervisor and the Data Owner.

k. Using licensable software without a license.

l. Circumventing or disabling user authentication or security of any computer/device, network or Scripps login or security safeguards.

m. Unauthorized decryption or attempts to decrypt any systems, passwords, or files.

n. Executing any form of network monitoring which will intercept data not intended for the user's computer/device unless part of the user's normal job duties. Port scanning, security scanning, and use of security monitoring tools are prohibited.

o. Establishing unauthorized direct Internet or non-Scripps wired or wireless network router connectivity from Scripps premises through DSL, ISDN, cable modem, or similar service provider vehicles.

p. Removing hardware components of Scripps computers/devices, such as hard drives.

q. Connecting any non-Scripps-owned computer/device into a Scripps wall port or otherwise attaching to data, voice, or wireless networks without explicit authorization from Scripps Information Services via a Help Desk ticket.

r. Storing confidential Scripps data on non-Scripps (personal) computers, mobile devices or removable storage devices.

s. Installing software or downloading executable programs onto Scripps-owned computers/devices without Information Services' pre-authorization or pre-authorization Software Request Forms through a Help Desk ticket to track license.

2. **The use of system administration privileges** is restricted to IT and BioMedical support staff with administrative responsibilities as described in the individual's job description. Any non-IT or BioMedical support staff requiring administrative privileges must be evaluated and approved through a risk

assessment process prior to the privileges being granted. Administrative privileges are audited and re-certified annually.

3. **Email and Communications Activities**

   a. Sending *unsolicited* email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). This includes posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

   b. Any form of harassment via email, telephone, texting, paging, whether through language, frequency, or size of messages.

   c. Unauthorized use, or forging, of email header information.

   d. Solicitation of e-mail for any other email address, other than that of the poster's Scripps login, with the intent to harass or to collect replies.

   e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

   f. E-mail, internet, or computer use for personal purposes unless *incidental*, as determined by your supervisor. This includes shopping, gambling, chats, bidding, ordering of personal items, online banking, investing, real-time stock price monitoring, playing of games.

   g. Use of Scripps systems or resources for political activities.

   h. Making fraudulent offers of products, items, or services originating from any Scripps login.

   i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

   j. Users should not send email outside of Scripps with confidential information either in the body or in attachments without password protecting attachments or otherwise ensuring email is encrypted through additional Scripps or third party processes as Scripps email is not automatically encrypted. See Confidentiality of Information policy S-FW-IM-0201.

   k. It is prohibited to use email or any other messaging capability, such as Instant Messaging (IM) or Chat to send any credit card primary account numbers (PAN) (numbers embossed and/or encoded on a plastic credit card), as this number identifies the Card issuer and the cardholder credit card account.

4. **Social Media Use**

   Personal web sites, blogs, wikis, and social networking sites (collectively, “Personal Sites”) have become prevalent methods of self-expression in our culture. Scripps respects the right of the employees to use these media (to “post” or “posting”) during their work or non-work time, subject to the guidelines set forth below. This policy is written to comply with applicable law and will not be interpreted in a manner that restricts the flow of concerted employee communication about terms and conditions of employment.

   a. Incidental use of Scripps systems to engage in personal posts or posting is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Scripps policy and does not interfere

with a user's regular work duties. All posts or posting from Scripps systems is subject to monitoring.

b. The Scripps Confidentiality of Information policy also applies to posts or postings on Personal Sites. As such, users are prohibited from revealing any Scripps confidential or proprietary information, trade secrets or any other material covered by Scripps Confidential Information policy when engaged in posts or posting on Personal Sites. Confidential and proprietary information of Scripps clients, partners, suppliers and other business and patient relationships may not be discussed or referenced, explicitly or otherwise, on a Personal Site without such party and Scripps express approval.

c. Employees may not post any material on any Personal Sites that is, or could be viewed as, malicious, obscene, defamatory, profane, libelous, threatening, intimidating, harassing or hateful to another person or entity regarding Scripps, its business, employees, partners, customers, users, suppliers, and competitors. Examples of prohibited conduct include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability or any other status protected by law or the Scripps Non-Discrimination and Anti-Harassment policy.

d. Employee personal posts on Personal Sites are individual expressions and not Scripps communications. Therefore, employees are personally responsible for their posts. Employee posts must clearly state that they are the employee's own opinions and are not the opinions of Scripps or its employees. That kind of disclaimer must be posted in a reasonably prominent place if the employee elects to post anything that relates to or references Scripps. Only authorized employees (for example, certain, expressly authorized employees in Marketing and Communications) are allowed to post on behalf of Scripps.

e. Employees may not violate trademark, copyright or any similar laws with their posting. Employees must obtain permission to use Scripps trademarks or to reproduce copyrighted material. Employees should respect all fair use, financial disclosure, securities and other laws when engaging in any posting activity.

E. Suspension or Removal of Access Privileges

Access to Scripps computers/devices, networks, email, or any requested services will be discontinued by Scripps upon termination of employment, contract expiration, end of service of a non-user, or violation of this policy. Access privileges may be suspended at any time by Scripps as may be required during a security or privacy violation investigation, at the request of Human Resources, or where deemed necessary to protect the integrity of Scripps networks and systems. When requested, users are expected to cooperate fully in any investigation of system abuse or security incidents. Failure to cooperate may be grounds for cancellation of access privileges and/or other disciplinary actions.

F. Reporting Information Security Incidents

Scripps implemented processes to help users promptly report events related to information security breaches and policy violations. Immediate reporting is essential,

as certain viruses or malicious activity could rapidly escalate and spread throughout electronic resources across the organization. These processes and descriptions of types of security incidents are described in Scripps Information Security Incident Reporting and Response, S-FW-IM-3005.

Information security incidents, including lost, stolen, or missing computers, removable storage devices, ID badges, and handheld devices must be promptly reported to the IS HELP DESK (858-678-8500) which will promptly alert the Security Incident Response Team (SIRT). The Scripps Patient Safety and Compliance Alertline (888-424-2387) can also be called when individuals choose to remain anonymous in reporting their concerns.

G. **Logging and Monitoring**

1. **Logging and Monitoring of Activity**. Scripps users must be aware that activities on Scripps computers/devices, application systems, network, Internet access, and e-mail usage are logged. These logs contain usage information, including, user identification, activity type, and date and time stamps. Logs may be routinely monitored, reviewed, and are available to designated authorized individuals responsible for investigation of complaints and monitoring compliance with Scripps policies.
2. **Requests for Activity Logs** regarding individual activity (including, but not limited to, internet usage, email content and usage, telephone usage, stored voice mails, surveillance camera records, and other similar information) requires written authorization by at least two (2) of the following three (3) parties:
    a. Legal Office representative;
    b. Human Resource Director and above (for information related to their business unit only); or
    c. Audit & Compliance Services Director and above.

    Managers with concerns about appropriateness of computer/device usage by users must first contact their site HR representative to determine whether the situation warrants extracting a log of the individual's computer/device activity and obtain pre-authorization from HR to request such logs.

III. PERSONNEL

This policy applies to all individuals using Scripps computing resources, including full-time users, part-time users, volunteers, contractors, vendors, physicians, and other non-users conducting business with, or for, Scripps and who have been granted access privileges by Scripps to information resources. This policy refers to all Scripps information resources, whether individually managed or shared, stand-alone or networked, and applies to all computer/devices and computer/devices communication facilities and services owned, leased, operated, or contracted by Scripps, and to all Scripps owned or managed data, regardless of its location and access duration. This includes equipment; mobile devices; software; operating systems; storage media; wired and wireless networks; dictating or transcription equipment; imaging equipment; biomedical devices; record archival systems; and network. Scripps logins providing electronic mail, internet browsing, and file transfer protocol (FTP) are the property of Scripps Health.

IV. ATTACHMENTS

A. Glossary of Terms

B. Personal Computer System Release of Liability Waiver

V. RELATED POLICIES

A. Business Associate Agreement Policy; S-FW-LD-1007

B. Confidentiality of Information (Patient, Financial, Employee and Other Sensitive and Proprietary Information); S-FW-IM-0201

C. Facsimile of Information Policy; S-FW-IM-2003

D. Harassment-Free Workplace Policy; S-FW-HR-0510

E. Health Information, Access, Use and Disclosure; S-FM-IM-0203

F. Information System Resources, Administering Access Privileges for Users; S-FW-IM-3002

G. Information Systems, Non-Employee Access; S-FW-IM-3004

H. Information Security Program Policy; S-FW-IM-3000

I. Information Security Incident Reporting and Response Policy; S-FW-IM-3005

J. Information Technology Project Approval and Management; S-FW-IM-3009

K. Information Technology Standards, Procedures, and Guidelines; S-FW-IM-9000

L. Research, Authorization, Use and Disclosure of Protected Health Information and Data Requests; S-FW-LD-1005

M. Scripps.org (Internet) Content, Management of; S-FW-IM-2002

N. Social Media Guidelines (see Confidentiality of Information)

O. Telecommuting Program; S-FW-HR-0706

VI. RELATED FORMS

A. Information System Resources (Mandatory Education); 100-8655-941SW

B. Request for Scripps Information Management Policy Exception; SW-IM-2001 A

C. Request for Software Installation; SW-IM-3009

D. Employee Automated Access Request Form (AARF)

E. Non-Employee Access Request Form; SW-IM-3004 A

F. Confidentiality and Non-Disclosure Agreement; 8650-061

G. Electronic Handheld Device Request Form; SW-IM-3006

H. Modem Access Request Form

I. Confidential Information Data Request Authorization Form; SW-IM-0203

J. Personal Computer Access to Scripps Network Security Safeguard Attestation; SW-IM-3004

K. Scripps Personal Computer System Release of Liability Waiver

VII. SUPERSEDED

Computer, Network, and E-mail Usage; S-FW-IM-2001 01/12

Authentication: The process of determining if someone (or something) is who (or what) it is declared to be and guarantees that the user is authentic. For example, a system user authenticates himself/herself through the user of their assigned user ID and password, Knowledge of the password is assumed to guarantee that the user is who she says she is.

Confidential Information: Information that includes, but is not limited to, PHI, PFI, patient records, personnel information, information regarding business plans and strategies, information gained from service on organizational or medical staff committees, and information gained from inquiries from families and friends of patients, other employees, the legal department, medical staff, external agencies or media. Confidential Information may be contained in any communication medium, including verbal, written, or electronic (e.g. facsimiles, e-mail, voicemail, pagers, text messages, photographs, social media such as Facebook, Twitter, U-Tube, Yelp), all which are subject to the provisions of the Scripps Information Patient, Financial, Employee and Other Sensitive and Proprietary Information; S-FW-IM-0201 policy.

Information Security Breach: Intentional or unauthorized, successful or unsuccessful activities or attempts to disrupt systems, access data that a system user is not an intended recipient, to log into a server or a computer session that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. Examples of such breaches include, but are not limited to, network sniffing, pinged floods, packet spoofing, interfering with or denying service to any user other than the user's computer/device (aka as denial of service), forged routing information for malicious purposes, guessing another person's password, trying to observe a system user while he/she enters the password (by shoulder surfing), accessing another user's email Scripps login without being authorized to do so, using any program, script, command, message with the intent to interfere with, or disable, a user's login session, via any means, locally or remotely, etc. These activities include using unauthorized tools to conduct such unauthorized activities.

Visitor Wireless Network: Wireless network established by Scripps Information Services as a courtesy service to patients, visitors, physicians, and third party vendors to connect their personal devices to the internet while on Scripps premises.

PERSONAL COMPUTER SYSTEM RELEASE OF LIABILITY WAIVER

I_____, offered to have Scripps Health conduct a computer security review of my personal computer related to a security event. I have temporarily provided my personal computer or hand held device to Scripps Health authorized staff members for the sole purpose of security review to determine if my personal computer was compromised resulting in the security event to Scripps. No software or data will be removed from my computer as part of this review. I understand that Scripps Health may use its third party contracted security partner to take a digital image of my personal computer/device for performing the security investigation. Scripps Health makes no representations or warranties with respect to this review. Consequently, I agree that I will hold Scripps Health harmless from any claims, demands or causes of action (collectively "Liabilities") arising out the security review. I understand that the computer/device will be returned to me on _____.

Please FAX completed form to 858-678-7209

Signature:_____ Date:_____
Print Name:_____ Phone:_____
Corporate ID_____
Facility:_____