I. PURPOSE: To establish the acceptable use of Scripps’ computer, email, and network resources.

II. POLICY

A. Internet, e-mail, network, and application system access is granted to individuals to carry out job functions and assigned duties to support clinical and business services.

B. Data created on Scripps systems is the property of Scripps. Scripps system users must have no expectation of privacy for activities carried out on Scripps and non-Scripps computers.

C. Scripps may monitor and audit equipment, application systems, network traffic and review logs at any time for security and network maintenance purposes or to ensure compliance with this policy.

D. All individuals who have access to Confidential Information are prohibited from using, discussing, or revealing such information in any unauthorized manner unless such information is required by the individual’s role and responsibilities.

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

1. Confidential data leaving Scripps must be protected through encryption or equivalent authorized mechanisms while in transit. Use encryption and other safeguards.

2. Keep passwords secure and do not share Scripps logins. Authorized users are responsible for the security of their passwords and Scripps logins.

3. 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 or by locking or logging-off when the computer/device is unattended. Refer to Computer, Session Pause, and Timeouts, S-FW-IM-3001.

E. 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.

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 is prohibited.

F. Users must use caution when opening e-mail attachments or when clicking on hyperlinks received from unknown senders which can harm the Scripps network or clinical and business computing resources.

G. Personal Devices

1. Personal devices or computers must be approved to connect to Scripps information, network, and application systems to conduct Scripps business. Users must consent to fully cooperate with any investigation in which their
personal device is reasonably suspected to have been compromised or involved in a security or privacy event.

2. 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 (Attachment B) must be signed.

3. Privileges to connect to the Scripps network with a personal device may be suspended or revoked if the user refuses to cooperate with any investigation deemed necessary.

4. Connecting a personal device in an unauthorized manner is prohibited.

H. 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.

I. Use of Social Media

1. Refer to Scripps Guidelines for the Use of Social Media, S-FW-IM-0201G when using Scripps e-mail resources, accessing the Internet from the Scripps network/ Scripps login, or posting while stating an affiliation with Scripps.

2. Personal postings should be done using a personal e-mail login (not Scripps e-mail or Scripps login).

3. Scripps respects the right of the employees to use social media during their work or non-work time, subject to the requirements set forth in this policy. 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.

4. Incidental use of Scripps systems to engage in personal posts or posting is acceptable, provided 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.

5. Employee personal posts on Social Media Sites are individual expressions and not Scripps communications. Employees are personally responsible for their posts and must clearly state that they are the employee’s own opinions and are not the opinions of Scripps or its employees. A similar type 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 (e.g. Marketing and Communications) are allowed to post on behalf of Scripps.

J. 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.

Refer to ATTACHMENT A: Prohibited Activities. The list 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. Specific users may be exempted from certain of these prohibited activities during the performance of their legitimate job responsibilities.
K. The use of system administration privileges is restricted to IS and Biomedical support staff with administrative responsibilities as described in the individual’s job description. Any non-IS 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.

L. Suspension or Removal of Access Privileges
1. 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.
2. 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 when 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.

M. Reporting Information Security Incidents
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 The Scripps Patient Safety and Compliance Alertline (888-424-2387) can also be called when individuals choose to remain anonymous in reporting their concerns. Refer to Scripps Information Security Incident Reporting and Response, S-FW-IM-3005.

N. 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. Logs may be routinely monitored, reviewed, and are available to designated authorized individuals responsible for investigation of complaints and monitoring compliance with Scripps policies.
1. 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)
   c. Audit, Compliance, & Information Security 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 Scripps entire workforce, including employees, volunteers, and contracted third parties having access to Scripps information. The policy also applies to medical staff members, residents, fellows and interns, employees of medical groups
contracted with the Scripps Medical Foundation and other affiliates that have access to Scripps Confidential Information.

IV. ATTACHMENTS
   A. Prohibited Activities
   B. Personal Computer System Release of Liability Waiver
   C. Definitions

V. RELATED PRACTICE DOCUMENTS
   A. Confidentiality of Information (Patient, Financial, Employee and Other Sensitive and Proprietary Information); S-FW-IM-0201
   B. Computer, Session Pause, and Timeouts; S-FW-IM-3001
   C. Harassment-Free Workplace Policy; S-FW-HR-0510
   D. Information Security Program Policy; S-FW-IM-3000
   E. Social Media Guidelines; S-FW-IM-0201G A

VI. RELATED FORMS
   A. Scripps Standards of Conduct; 100-NS8631-105SW
   B. Confidentiality and Non-Disclosure Agreement; SW-IM-0201 C
   C. Employee Automated Access Request Form (AARF)
   D. Non-Employee Access Request Form; SW-IM-3004 A

VII. SUPERSEDED
     Computer, Network, and E-mail Usage; S-FW-IM-2001, 8/17
The following are prohibited activities: **Social Media Use**

- Revealing Scripps confidential or proprietary information, trade secrets, or any other material covered by Scripps Confidential Information policy when posting on Social Media Sites.

- Revealing confidential and proprietary information of Scripps patients (including patient photos), clients, partners, suppliers and other business and patient relationships without such party and Scripps express approval.

- Posting any material 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 Harassment-Free Workplace, S-FW-HR-0510.

- Posting on behalf of Scripps without authorization

- Use of Scripps systems or resources for political activities.

- Use of Scripps systems or resources to solicit money for fundraising. No staff may solicit money for fundraising without the express approval and oversight of Scripps Foundation.

- Violating trademark, copyright, or any similar laws with 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.

The following are prohibited activities: **Email and Communications**

- 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), including posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

- Any form of harassment via email, telephone, texting, paging, instant messaging, or posting whether through language, frequency, or size of messages.

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

- Use of email or instant messaging 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

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

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

- 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.

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

- Use of Scripps systems or resources for political activities.

- Use of Scripps systems or resources to solicit money for fundraising. No staff may solicit money for fundraising without the express approval and oversight of Scripps Foundation.

- Sending email outside of Scripps with Protected Health Information (PHI) or 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. Scripps email is not automatically encrypted.
The following are prohibited activities: System and Network Use

<table>
<thead>
<tr>
<th>Prohibited Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.)</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Attempting to gain access to another’s password or information or using someone’s already logged-on session.</td>
</tr>
<tr>
<td>Breaching security or causing intentional disruptions to network communication.</td>
</tr>
<tr>
<td>Circumventing or disabling user authentication or security or of any computer/device, network or Scripps login or security safeguards.</td>
</tr>
<tr>
<td>Connecting any non-Scripps-owned computer/device or network device into a Scripps wall port or otherwise attaching to data, voice, or wireless networks without explicit authorization from Scripps Information Services.</td>
</tr>
<tr>
<td>Establishing unauthorized direct Internet or non-Scripps wired or wireless network router connectivity from Scripps premises.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Introduction of malicious programs into the network or server.</td>
</tr>
<tr>
<td>Providing information about, or lists of, Scripps users to third parties without authorization by your supervisor and the Data Owner.</td>
</tr>
<tr>
<td>Removing hardware components of Scripps computers/devices (e.g. hard drives)</td>
</tr>
<tr>
<td>Revealing your Scripps login session password to others or allowing others to use your Scripps login and password.</td>
</tr>
<tr>
<td>Storing confidential Scripps data on non-Scripps (personal) computers, mobile devices, or removable storage devices.</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Unauthorized decryption or attempts to decrypt any systems, passwords, or files.</td>
</tr>
<tr>
<td>Using a Scripps computer/device to view, acquire, store, or disseminate data that is illegal, pornographic, or in non-compliance with the Scripps' policy Harassment-Free Workplace, S-FW-HR-0510.</td>
</tr>
<tr>
<td>Using licensable software without a license.</td>
</tr>
<tr>
<td>Using Medical Devices/systems network access or applications for other than appropriate clinical purpose.</td>
</tr>
<tr>
<td>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 &quot;pirated&quot; or other software products that are not appropriately licensed for use by Scripps.</td>
</tr>
</tbody>
</table>
PERSONAL COMPUTER SYSTEM RELEASE OF LIABILITY WAIVER

1. I, [name]___________________, offered to have Scripps Health conduct a computer security review of my personal computer related to a security event.

2. 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 a security event to Scripps.

3. No software or data will be removed from my computer as part of this review.

4. 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.

5. Scripps Health makes no representations or warranties with respect to this review.

6. 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.

7. I understand that the computer/device will be returned to me on [date]______________.

Please FAX completed form to 858-678-7209

Signature: _________________________ Date: ____________________
Print Name: ______________________ Phone: ___________________
Corporate ID: _______________________
Facility: _________________________
A. **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 use of their assigned user ID and password, knowledge of the password is assumed to guarantee that the user is who she says she is.

B. **Information Security Breach**: Intentional disruption of information systems, inappropriate/unauthorized accessing of data or logging into a computer session/server. Examples include, but are not limited to:
   - Accessing another user’s email Scripps login
   - Using any program, script, command, message with the intent to interfere with, or disable, a user’s login session
   - Guessing another person’s password, trying to observe a system user while he/she enters the password
   - Forged routing information for malicious purposes
   - Network sniffing, pinged floods, packet spoofing

C. **Security Incident**: the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

D. **Visitor Wireless Network**: Wireless network established by Scripps Information Services as a courtesy service to connect personal devices to the internet while on Scripps premises.