Shriners Hospitals for Children
Remote Access Acceptable Use Policy (RAAUP)

Acknowledgement

I. Definition and Overview

The purpose of this policy is to provide guidelines for remote access to SHC’s protected network computing infrastructure. Remote access is defined as all access to SHC computing and network systems accomplished by means other than the SHC internal networks. Some examples of remote access methods are: access from SHC owned, employee owned and third party owned equipment including, but not limited to, offsite personal computers, laptop computers, personal digital assistants (PDAs), Blackberry devices, etc. This policy applies to all employees, officers, Board members and others who are approved to utilize SHC’s remote access. These policies are designed to minimize potential exposure to SHC from damages which may result from unauthorized use, loss of sensitive or confidential information, intellectual property, damage to public image, etc. SHC’s remote access is intended to provide a resource to be used in a manner consistent with responsible corporate business practices and the Mission of SHC.

II. Policy Statement

A. Remote access must be used for official SHC business and purposes exclusively and will be governed by all applicable SHC policies, specifically TEC.005(1), TEC.005(2), and TEC.010 and TEC.016.

B. Remote access administration will be centralized at SHC’s headquarters.

C. Remote access will be available to approved salaried or exempt employees, members of the Board of Governors and members of the Joint Boards who require such access to enhance their ability to carry out duties associated with SHC.

D. Remote access to email will be limited to salaried or exempt employees, members of the Board of Governors and members of the Joint Boards except in special cases that will require approval by the Headquarters level.

E. Remote Access To SHCIS only (RATS) will be as governed by policy TEC.016.

III. Approval Procedure

A. The requester must read, initial and sign this document and the “Remote Access Request Form” (RARF) with a witness.

B. The requester’s supervisor must approve the “Remote Access Request Form” (RARF).

C. A Human Resources representative must approve the “Remote Access Request Form” (RARF), verifying the exempt status of the requestor.

D. At the hospitals, the hospital Administrator must approve the “Remote Access Request Form” (RARF).

E. At Headquarters, the Vice President of Information Services must approve the “Remote Access Request Form” (RARF) for hospital and HQ requesters.

F. The “Remote Access Request Form” (RARF) may be faxed to HQ Information Systems for approval. The originals of this document (RAAUP) and the “Remote Access Request Form” (RARF) will be as governed by policy TEC.016.
(RARF) must be stored in the requester’s Human Resources file and a copy must be distributed to the requester.

G. The requester will be notified by email upon approval or denial of the request.

IV. Responsibility and Use

A. Great care must be taken to protect the integrity of the remote access system and SHC’s sensitive and confidential information.

B. Lost smartcards, access tokens and other authentication must be reported to local IS immediately.

C. Secure remote access must be strictly controlled. At no time should one provide their login, password or PIN to anyone else.


E. Remote access must be limited to the length of time necessary to accomplish essential tasks.

F. Care must be taken to prevent the unintentional release of proprietary information to unauthorized persons during a remote access session.

G. A remote access connection must never be left connected while unattended.

H. Remote access sessions must be properly closed before leaving a computer used for access.

I. Any generated hardcopy must not be left behind or accessible to unauthorized persons.

I acknowledge that I have received a copy of the foregoing Remote Access Acceptable Use Policy (RAAUP), read it carefully, understand it, and agree to abide by it.

______________________________  __________________________
Requester                                      Witness

______________________________  __________________________
Date                                          Date
**REMOTE ACCESS REQUEST FORM (RARF)**

<table>
<thead>
<tr>
<th>SHC Location:</th>
<th>Department:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requestor (Print):</td>
<td>Date:</td>
</tr>
<tr>
<td>Supervisor (Print):</td>
<td>Date:</td>
</tr>
</tbody>
</table>

If the requestor is a non-exempt (hourly paid) employee, please attach a completed copy of the Human Resources “Request for Exception” form and “Non-Exempt User Remote Access Agreement”.

The requester, by signing and submitting this form, certifies that he/she has received a copy of, signed for, read and fully understands the Remote Access Acceptable Use Policy (RAAUP) Acknowledgement, which is attached hereto, the HIPAA and SHC Security Policies and Procedures and the Internet Acceptable Use Policy (IAUP) and hereby agrees to abide by the conditions set forth. The requester also certifies that he/she understands and agrees that violation of the RAAUP, the SHC Security Policies or the IAUP could result in appropriate disciplinary action up to, and including termination. In addition, the requester understands that in cases where damages have been caused or laws violated, SHC reserves the right to pursue legal action.

**IMPORTANT:** The existence of SHC business related information on the user’s non-SHC owned computing device could expose that device to subpoena or other discovery should such information come under litigation.

- [ ] Full System Access (Requires SHC owned computer with Smartcard.)
- [x] SHCIS Only Access (RATS - Remote access limited to SHCIS for non-SHC owned computer: requires access token. USER MUST MEET ALL CRITERIA AND REQUIREMENTS IN POLICY TEC.016.)
  - PLEASE INCLUDE YOUR SHCIS LOCATION CODE - AVAILABLE FROM YOUR LOCAL IS DEPT - IN THE BUSINESS JUSTIFICATION AREA BELOW.
- [ ] Email Only Access (Remote access to non-PHI, non-sensitive / non-confidential email: does not require SHC owned computer, smartcard or access token.)
- [x] Other (Please describe)  PACS

**Business Justification for Remote Access**

<table>
<thead>
<tr>
<th>Requester’s Title (Print):</th>
<th>Date Signed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requester’s Signature:</td>
<td></td>
</tr>
<tr>
<td>Witness:</td>
<td></td>
</tr>
<tr>
<td>Supervisor’s Signature:</td>
<td>Date Signed:</td>
</tr>
<tr>
<td>Human Resources’ Signature:</td>
<td>Date Signed:</td>
</tr>
<tr>
<td>Administrator’s Signature (N/A if Requester is an HQ employee):</td>
<td>Date Signed:</td>
</tr>
</tbody>
</table>

**Corporate Use Only**

<table>
<thead>
<tr>
<th>VPIS Signature:</th>
<th>Date Signed:</th>
</tr>
</thead>
</table>