


# RIVERSIDE UNIVERSITY HEALTH SYSTEM

## Housewide

		Document No: 712	Page 1 of 5
<b>Title:</b>  Computer Hardware and Software – Access, Use and Security	<b>Effective Date:</b>  5/6/2025	<input checked="" type="checkbox"/> RUHS – Community Health Centers <input checked="" type="checkbox"/> RUHS – Hospital Based Clinics <input checked="" type="checkbox"/> RUHS – Medical Center <input type="checkbox"/> Departmental	
<b>Approved By:</b>    Jennifer Cruikshank CEO/ Hospital Director		<input checked="" type="checkbox"/> Policy <input checked="" type="checkbox"/> Procedure <input type="checkbox"/> Guideline	

### 1. POLICY. The policy of RUHS is to:

- 1.1 Ensure the security and privacy of the information stored and/or transmitted through the RUHS computer hardware, software, networks, internet, and email system.
- 1.2 Establish and enforce workstation standards and safeguards for user access to the RUHS computer systems and applications.
  - a. RUHS reserves the right to amend policies and guidelines without notice in accordance with applicable federal, state, and local laws and regulations.

### 2. DEFINITIONS

- 2.1 Information Technology (IT). A computer system comprising hardware and software used to store, process, and maintain data electronically. This includes software link to multiple users via RUHS networked servers.
- 2.2 Information Services Department (IS). The department responsible for managing electronic systems and data stored, processed, and maintained in the RUHS environment.
- 2.3 Security Standards. Reasonable safeguards required by federal, state, and local laws/regulations to protect the confidentiality, integrity, and availability of RUHS systems and data.
- 2.4 System Access Request (SAR) form. A required form to obtain access to RUHS computer systems and applications. The form specifies requested access and can be found under the RUHS Intranet, Information Services (IS), Help Desk, Services Desk Forms.
- 2.5 Workforce Members. Employees regular or temporary, physicians, volunteers, students, residents, interns, and other persons whose performance of work is conducted at a RUHS facility.

### 3. GUIDELINES

#### 3.1 Authorized Use and Access

Only authorized workforce members approved through the SAR process will be granted access to computer hardware, software, and networks for the delivery of services. RUHS retains the right to monitor all RUHS systems to ensure proper use.

- a. Use of the RUHS systems implies agreement to the terms of this RUHS policy.
  - RUHS users have no expectation of privacy when using RUHS-owned hardware, software, and network, including email.
- b. Authorized workforce members must be acting within the scope of their employment or contractual relationship with RUHS.
- c. Users will receive specific usernames and passwords, and agree to:
  - Not to share their credentials with anyone, including coworkers, supervisors, and/or managers.
  - To take appropriate steps to prevent the loss or theft of their credentials.
- d. Users must implement reasonable safeguards to protect the integrity, confidentiality, and availability of systems and applications.

#### 3.2 Use prohibitions include but are not limited to:

- a. Sending or sharing any sensitive or confidential information with unauthorized individuals.
- b. Making copies of any sensitive or confidential data without authorization.
- c. Installing non-standard software or hardware that has not been approved by RUHS IS Department.
- d. Attaching non-authorized personal mobile devices to RUHS private/internal network
- e. Attaching non-authorized personal computers to RUHS private/internal network without written permission from RUHS IS Department.
- f. Using network resources to play or download games, music, or videos that are not in support or under the scope of employment at RUHS for business or educational functions.
- g. Leaving workstations unattended without locking or logging out of the workstation.

- h. Leaving workstations unattended without locking or logging out of the workstation.
  - i. Using RUHS network resources for, or in, support of unlawful activities as defined by federal, state, and local law.
  - j. Utilizing network resources for activities that violate conduct policies as established by RUHS and the County of Riverside.
  - k. Users agree that Protected Health Information (PHI) will not be stored or maintained on electronic remote access devices to be taken off site from any RUHS location including, but not limited to, laptop computers or other portable electronic devices, flash drives, USB, etc.
  - l. Users agree any such person with access, authorized or not, to RUHS computer system(s) who damages RUHS hardware or software due to having installed, downloaded, or upgraded unauthorized software will be responsible for the cost of the repair. Any computer related purchases of goods or services will be coordinated through the RUHS IS Department.
- 3.3 Access to RUHS Networked Computer Systems. Workforce members requesting access to the RUHS computer system must complete and submit a SAR form to the IS Department for processing.
- 3.4 Workstation Security. Workforce members will take reasonable steps to protect the integrity and confidentiality of information stored and maintained on the RUHS computer system.
  - a. Users shall log-off or lock their workstations prior to walking away and leaving their workstation unattended.
  - b. Screen savers shall not be de-activated, where installed.
  - c. Workstations shall be placed in the most secure area possible, preferably behind locked doors or other secured areas of RUHS.
  - d. Monitors shall be positioned in such a way that they are not easily viewed by any passerby.
  - e. Screen protectors shall be utilized in areas where there is a probability of unauthorized individual(s) viewing electronic Protected Health Information (ePHI).
- 3.5 Email Use. Email shall be used for communication which will assist in the efficient performance of job-related tasks. Email shall not be used for personal reasons.
  - a. Any information communicated via email shall be limited to only the minimum necessary information and, unless encrypted, shall not include protected or sensitive information (i.e. PHI/PII/Confidential).
  - b. A system generated confidentiality statement is automatically added to emails sent outside the RUHS domain.
  - c. Users are encouraged to “Archive” or create separate file folders to store email needed for future reference. All items in the email “Deleted Items” folder and “Conversation History” folder will be purged in 24 hrs.
- 3.6 Email Prohibitions. Emails should be used only to send courteous, professional, and businesslike communications. The following list provides examples of information that may **not** be transmitted via email:

- a. Patient information (unless encrypted).
    - Including names in any format, medical record numbers, date of birth, account numbers, social security numbers, etc.
  - b. Confidential material to an unauthorized recipient.
  - c. Unsolicited junk email, advertising, items-for-sale postings, or chain letters (e.g. “spam”).
  - d. Any communications that violate County and/or RUHS conduct policies.
- 3.7 Network Drives. The RUHS Network is the safest storage choice for business-related documents and/or confidential information.
- a. Business related documents and confidential information shall be saved to a local network drive Microsoft OneDrive/SharePoint. Such documents shall not be saved to any storage media outside of the network (i.e., “C” or “D” drive, USB devices, or any other portable devices).
  - b. Storing or sharing files through the Internet (i.e. Yahoo Briefcase, Google Documents, Drop Box, or any similar service) is strictly prohibited, with the exceptions of Microsoft OneDrive and Box.
- 3.8 Purchases of Computer Hardware, Software, Applications, or Other Computer Tools. Purchases of any computer hardware, software, applications, or other computer tools must be approved by IS Department prior to submittal for purchase. A Request for Supplies or Services Form must be completed.
- 3.9 IT Equipment Relocation
- a. IT equipment relocation requests must be submitted to IS for processing and must include Department manager or Administrator approval.
  - b. The request will be sent to IS for review and approval.
    - IS teams that may be expected to review are Desktop Support, Networking, and/or Communications.
    - IS will sign off on the Move Request form and notify the requestor.
  - c. Once approval is received from the appropriate IS teams, requestor will be authorized to facilitate the move according to the relocation requirements indicated in the Move request form.
- 3.10 Reports of Policy Violations or Computer Concerns. Any suspicion of violations to this policy or suspicions of computer virus, worm, or other malicious malware that has infiltrated the computer workstation shall be reported immediately to the IS Help Desk at (951) 486-HELP (486-4357).

#### 4. REFERENCES

- 4.1 Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 4.2 Board of Supervisors Policy A-50, Electronic Media and Use Policy

**Document History:**

<b>Prior Release Dates:</b> 3/2000, 4/2005, 1/2015, 10/1/2018, 10/10/2019		<b>Retire Date:</b> N/A	
<b>Document Owner:</b> Information Services		<b>Replaces Policy:</b> N/A	
<b>Date Reviewed</b>	<b>Reviewed By:</b>	<b>Revisions Made Y/N</b>	<b>Revision Description</b>
3/24/2025	RUHS ISO	Y	<ul style="list-style-type: none"><li>Standardized term for IS to include all Information Services departments.</li><li>Corrected network storage location guidance.</li><li>Modified section 3.9 to updating review/approval requirements.</li><li>Removed non-relevant policy H-11</li><li>Removed A-38 – rescinded</li><li>Remove A-58 – non-relevant policy</li></ul>
4/1/2025	PAC	N	