Status **Active** PolicyStat ID **9849983**

Implementation	05/2021
Last Reviewed	05/2021
Effective	05/2021
Last Revised	05/2021
Next Review	04/2024

Owner	Adam Zoller: SVP Chief Info Security Ofcr
Policy Area	Cybersecurity
Applicability	Providence Systemwide + PGC

PSJH-EIS-950.08 Acceptable Use Standard - Corresponds to: PSJH-EIS-950 Information Security Management Policy

Purpose:

This standard is a mandatory course of action or rules that give the formal policy support and direction. It establishes PSJH requirements for acceptable use of computer equipment and resources.

Definitions:

Confidential Information, for the purposes of this standard, is any information, regardless of format, about patients, employees, students, residents, or business operations that PSJH deems should not be available without specific authorization. Loss or inappropriate access to this kind of data could harm patients, PSJH reputation and ability to do business. Confidential information includes but is not limited to PHI, ePHI, PII, card holder data (PCI), employee information, financial information and any other information that is intended for limited internal use by PSJH.

For the definition of terms not specifically defined above, please refer to PSJH-RIS-850.05, Privacy and Security Glossary.

Policy Linkage:

System Policy: PSJH-EIS-950, Information Security Management Policy.

Standard:

This technical standard and/or detailed procedure is an extension of the policy linked above. For scope and applicability of this standard, refer to the parent policy. The standard is in place to protect the confidentiality, integrity and availability of PSJH information and information systems. Inappropriate use

exposes PSJH to risks including virus attacks, compromise of network systems and services, and litigation.

Requirements:

A. **General requirements for the use of PSJH information and information systems**

1. All authorized PSJH workforce members have a responsibility to protect PSJH information and information systems. Users must only access PSJH information and information systems for which they are authorized. Misuse of PSJH information and information systems may put the organization, data, and patients at risk.
2. Personal use of PSJH resources is a limited privilege. Limited personal use of information systems is permitted with the following restrictions: usage must be reasonable, ethical and legal and usage must not interfere with any workforce members' responsibilities or productivity. PSJH Information Services may limit the quantity and/or type of personal-use files stored on information systems or networks.
3. Prior to accessing PSJH information and information systems users are required to acknowledge and agree to follow the Acceptable Use Standard. Users holding an employment contract or who work through a third-party contract between PSJH and the user's third- party employer are required to acknowledge and agree to follow an appropriate acceptable use agreement maintained by Contracting and Procurement. Failure to acknowledge this agreement or violation of this agreement may result in denial of access to PSJH information and information systems.
4. Users connecting an approved mobile device to PSJH information systems must follow the requirements in the standard 951.01, Information Technology Asset Management. The mobile device must meet all the required security controls. This applies to all devices whether personally owned or issued by PSJH.
5. PSJH reserves the right to monitor all use of PSJH information systems and all access to PSJH electronic data. Users of PSJH information systems have no expectation of privacy with regards to content or use of electronic communications or data within any PSJH information system.
6. PSJH paper documents, computers, and mobile storage and computing devices must be protected from loss, theft, unauthorized use, disclosure, modification, or destruction. They must be physically secured when taken off site.
7. All authorized users must take all reasonable steps to protect the privacy and security of confidential patient and confidential business information. In order to minimize the potential for loss and disclosure, confidential patient information, whether in paper or electronic format, must always be in the possession of the PSJH employee or agent, or in a secure location.
8. All users are required to promptly report the loss, theft, unauthorized use, unauthorized disclosure, unauthorized modification or unauthorized destruction of paper documents, electronic data, computers, or mobile storage and computing devices by notifying the Information Service Desk.
9. All authorized users are required to cooperate with PSJH investigation or

remediation efforts related to information security incidents.

10. All authorized users must follow these and all the requirements of PSJH policies. Violation of these requirements may result in disciplinary action up to and including termination of employment or termination of contractual arrangement(s) with PSJH. Violations may subject individuals to civil and/or criminal penalties.
11. Nothing in this policy is intended to restrict employees from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

B. **Terms of Acceptable Use:** Acceptable use of PSJH information and information systems by authorized users is generally described below:

1. **User Access**

a. Users are only permitted to use their own PSJH-assigned IDs and must not use the credentials that were assigned to other users.

b. Users are accountable to protect the confidentiality their unique IDs and passwords.

c. Users must not employ the same password used for PSJH accounts to access other non-PSJH accounts (e.g. personal ISP account, website accounts, etc.).

d. Users may not share their passwords with anyone.

e. Passwords must follow PSJH password requirements.

f. Users must not print or store passwords insecurely. Passwords must not be written down.

g. Users must inform the Information Service Desk and must change their password, and other credentials, if they believe that their passwords are compromised.

h. Users are not allowed to access PSJH information or information systems for which they have not been authorized.

i. The use and handling of mobile storage and computing devices is restricted to those individuals who are authorized to access these devices.

j. Users accessing confidential information (including Protected Health Information) are only authorized to access the minimum information necessary to do their jobs.

k. When accessing PSJH confidential information from an off-site location, users must use reasonable safeguards to ensure that the work session cannot be viewed by unauthorized individuals.

l. Users must secure all applications (log out/lock) when leaving a workstation unattended or accessible to unauthorized individuals (e.g., patients, visitors).

m. Users may only use approved remote access services meeting PSJH security requirements.

n. Authorized users may not allow any unauthorized user to access PSJH information systems or data.

o. Shared workstations (e.g., "auto-login" workstations) must be configured with a unique network identification that is automatically logged on to the PSJH network. Access to any confidential information from such shared workstation must require individual user authentication.

p. Users must not store confidential information locally on shared workstations.

2. **Computing Devices and Software**

a. No personal devices are allowed to be connected to the PSJH internal networks unless specifically approved by Information Services.

b. The use of all electronic storage media/portable storage devices must follow PSJH standard EIS 951.01, Information Technology Asset Management.

c. Only software and applications authorized by Information Services and have passed a security review by Information Security Services may be installed on a computing system or a mobile computing device. PSJH standard 950.05, Vendor Security Risk Management.

d. An automobile is not considered a secure location and should not be used to store confidential information, papers or mobile computing or storage devices. A mobile computing device should never be left unattended in an automobile. In some circumstances it may be preferable for the user to leave an appropriately secured tablet or laptop computer in a vehicle rather than removing it from the vehicle. Examples of such circumstances include:

i. The vehicle will only be unoccupied for a few minutes in a well-observed location.

ii. Removing the laptop or tablet from the vehicle will expose the device to more likelihood of loss or theft due to a crowded public venue.

iii. It is infeasible to take the laptop or tablet due to physical constraints. ***In such circumstances, a PSJH laptop or tablet may be left in an automobile as long as the following conditions are met:***

iv. The device must be stored out out-of-sight (e.g., under a seat or in the trunk).

v. The vehicle must be locked.

e. Transportation of PSJH computing devices (e.g. laptops, tablets, Smartphones, storage devices) outside of the United States requires approval, and is subject to the following restrictions:

i. Under no circumstances must a PSJH computing device be transported to a country that has a United States State

Department Travel
Warning: http://travel.state.gov/content/passports/en/alertswarnings.html

ii. PSJH does not allow permanent remote working outside of the United States. When PSJH workforce members seek temporary remote work outside of the United States, PSJH computing devices may be transported to countries not under a State Department Travel warning, with written approvals from System Director (or above), Division or Line of Business Chief Human Resources Officer, Chief Risk Officer, and Senior Corporate Counsel of Department of Legal Affairs (DLA). The written approvals must be obtained prior to traveling. Each such request will be evaluated on a case-by-case basis.

iii. Any PSJH computing device authorized for transport outside the United States is required to meet the following conditions:

a. Transport of the device to the foreign country must be required for conducting PSJH business.

b. PSJH computing devices must be encrypted.

c. PSJH Authorized VN connections and monitoring tools shall be turned on at all times.

d. Any non-required confidential information must be removed from the device prior to travel abroad.

e. Any inspections, tampering or loss of custody of the device must be immediately reported to the Enterprise Information Services Operations Center.

f. The device must not be packed in checked baggage during travel.

f. Papers containing confidential information and mobile storage and computing devices must not be checked with baggage on commercial transportation (e.g., airline, train).

g. Under no circumstances are workforce members to use mobile computing devices, mobile phones or pagers while operating a motor vehicle unless such use is hands- free, meets applicable laws and regulations and does not interfere with the safe operation of the vehicle.

h. PSJH computers must comply with a standard desktop build managed by Information Services. This includes but is not limited to the installation of current service packs, current virus protection software, client firewall and firewall configuration, and password protection.

i. Users may not modify or attempt to remove or disable PSJH standard software and hardware security controls and system configurations of PSJH computers except as authorized by Information Services.

j. Computing devices must connect with PSJH infrastructure (either locally

or remotely via VPN) at least monthly in order to receive automated maintenance and inventory services.

3. **Confidential Information**
    a. When electronic confidential information is stored, transported or transmitted outside PSJH facilities it must be encrypted.
    b. Confidential information may be used, accessed or disclosed only to those who have a need to know. Only the minimal necessary amount of confidential information must be used, accessed or disclosed.
    c. Any portable storage or computing device containing PSJH confidential information must be encrypted, and password protected.
    d. Confidential information must deleted or removed from the PSJH information systems in accordance with the PSJH-RIS-715 Records Retention and Disposal policy.
    e. PSJH information classified as confidential or internal use must not be printed at off- site locations without the appropriate level of PSJH management approval.
    f. All use of PSJH confidential information off site must follow PSJH standard 951.01, Information Technology Asset Management relating to device and media handling, storage and transport.
    g. Paper documents and storage and computing devices containing confidential or internal use information must be secured from unauthorized access or use while awaiting destruction and must be destroyed in accordance with PSJH standard PSJH EIS 951.02, Data Handling and Destruction.

4. **Confidential Patient Information:** Authorized users providing patient care in a home setting must secure all confidential patient information by meeting the following requirements:
    a. Take only the minimum necessary information for the care of current patients located off site.
    b. Once a patient is no longer under the care of PSJH, their confidential information must be deleted from mobile devices and all associated paper documents must be disposed of in accordance with PSJH standard PSJH EIS 951.02, Data Handling and Destruction.
    c. When involved in patient care in a home setting, confidential patient information must be protected from unauthorized access.
    d. Authorization by a supervisor is required for an employee to store confidential patient information in their home. Authorization is to be based on particular circumstances or a particular job description.
    e. Patient confidential information (ePHI) stored temporarily at home must be kept in a secure location such as a locked drawer, cupboard or office.

5. **Internet Use**

a. All use of social media (e.g., social networking) must be in accordance with PSJH- COMM-604 Electronic Social Media policy.

b. PSJH blocks categories of inappropriate Internet sites because of information security risks or as requested by leadership. Purposeful attempts to access blocked sites are a violation of this policy.

c. PSJH blocks Internet cloud service sites for sharing documents and data. Internet website services or cloud services refer to any resource that is provided over the Internet. Examples of cloud services include, but are not limited to:

    i. Any site on the Internet asking to create a user name/password and login.

    ii. Any site where entering patient information through a website form. This includes sites set up by medical device manufactures and medical software companies.

    iii. Document sharing or note taking sites such as Dropbox, Google docs, and Evernote.

    iv. Any Non-PSJH system that stores PSJH data must be approved by Information Security and have an appropriate contract and/or Business Associate Agreement.

    v. Workforce members are subject to Internet filtering and must use approved methods to access the Internet from PSJH facilities.

    vi. Authorized users are responsible to ensure that Internet content accessed via PSJH information systems is appropriate for the workplace. Internet access may be limited or disabled at the discretion of PSJH.

6. **Intranet and Extranet Use**

    a. PSJH intranet, extranet, and other collaborative tools are intended for PSJH business purposes only.

    b. External parties are not allowed to connect to the PSJH intranet unless it is with express permission of the appropriate level of PSJH management. Permission must be granted via a formal agreement/contract to address specific business needs.

    c. Confidential information posted to the intranet or extranet is subject to the requirements of the Confidentiality Policy (available on the HRPortal).

    d. Access to the PSJH extranet must only be provided to address particular business needs of external parties and PSJH.

7. **Electronic Communication**

    a. PSJH regularly monitors electronic communications on its systems including PSJH e-mail and instant messaging communications. Sending confidential information through Internet instant messaging is prohibited.

b. PSJH workforce members are not permitted to use third-party e-mail providers (e.g., personal e-mail accounts) to conduct PSJH business.

c. Users must ensure information contained in all postings, e-mail messages, or any other form of electronic transmission is accurate, appropriate, ethical, truthful, and lawful.

d. Users who have been delegated access to another person's electronic information e.g., e-mail, and calendar, must only access the information when needed.

e. Users may only subscribe to list server discussion groups that are specifically job- related. Legitimate list server subscribers are expected to maintain PSJH confidentiality guidelines in all list server discussion correspondence. When participating in list server discussion groups the following disclaimer must be attached to the subscriber's post*: The views and opinions expressed do not necessarily state or reflect those of Providence St. Joseph Health and its Affiliates. PSJH assumes no liability or responsibility for the accuracy, completeness, or usefulness of the information communicated*.

f. Electronic communications including e-mail can be retrieved regardless of whether the sender and receiver have deleted their copies.

g. User e-mail accounts will be deleted upon notification of termination of employment or contract with PSJH. Management may request transfer of mailbox contents prior to termination. PSJH may retain mailbox contents as needed.

h. E-mail is a communication tool and is not to be used as a storage mechanism for information. Information subject to specific retention requirements should be stored separately in a suitable electronic or paper system.

i. To prevent viruses, malware and other disruptions to PSJH information systems, users must avoid opening suspicious e-mails and accessing suspicious or inappropriate websites.

8. **Personally-Owned Devices**

a. Personally- owned devices must meet PSJH security requirements and may not connect to PSJH information systems or store PSJH confidential information unless authorized by Information Services.

b. Workforce members will be authorized to connect to PSJH systems or networks with an approved smartphone, tablet/i-Pad device only with the appropriate PSJH management approval.

c. Personally-owned devices connecting to the PSJH internal network must have current anti-virus installed, a method for receiving periodic operating system and application patches, and secure storage for PSJH information.

d. Personally-owned devices may only be used to access PSJH confidential information through approved access methods.

e. Any approved smartphone must support the following security controls before connection to PSJH networks is allowed:
    i. PSJH device administrators must have the ability to apply or configure appropriate device security controls.
    ii. A password or PIN must be enforced on the device.
    iii. Device passwords or PIN must have a minimum length of 4 characters.
    iv. Data on the device must automatically be erased after 10 failed authentication attempts or the device must lock out further authentication attempts.
    v. Devices must be configured to password lock after a maximum of 10 minutes of inactivity.
    vi. PSJH information classified as confidential or internal use must be encrypted.

f. PSJH specifically forbids the transfer of confidential information to user-owned storage or computing devices unless in accordance with PSJH policies and control standards.

9. **Prohibited Usage:** Prohibited communication activities include but are not limited to:

a. Creating or distributing discriminatory, harassing or other threatening messages or images. Caregivers encountering or receiving this kind of material must immediately report the incident to their supervisor.

b. Creation, storage or distribution of unacceptable content including, but not limited to, sexual comments or images, pornography, racial slurs, hate materials, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

c. Sending chain letters, broadcasting messages unnecessarily, sending messages repeatedly, and excessive or frivolous use of electronic communication technologies.

d. Communicating messages that denigrate, defame, or slander the products or services of PSJH or other entities or individuals.

e. E-mailing or otherwise sending confidential information to a personal e-mail account or Internet storage service.

f. Violation of the copyright or trademark law.

g. Violation of confidentiality or non-disclosure agreements.

h. Installation of software not authorized by Information Services.

i. Violation of licensing agreements.

j. Gambling, unlawful activity or any activity inconsistent with PSJH core

values.

k. Representing personal views as those of PSJH, including unauthorized use of the official logo.

l. Attempting to gain unauthorized access to a computer system of another organization or person.

m. Impersonating another person when sending email messages.

n. Deliberately jeopardizing the security of any PSJH information system.

o. Engaging in any conduct that is contrary to, or inconsistent with, the mission and values of PSJH.

10. **Recording Devices in the Workplace**

    a. Those working on behalf of PSJH must not record, monitor, or otherwise intercept the communications or activity of anyone through the use of any electronic, mechanical, or other recording devices except for official business use.

    b. Camera or mobile devices that have built in recording capability may be used for personal communication/assistance in appropriate areas. The recording capability of such devices must not be used in business/clinical areas without prior authorization.

Regulatory and Contractual Requirements:

The security of confidential information (including electronic Protected Health Information (ePHI)) is of particular importance. Violations of provisions of HIPAA can damage PSJH's reputation as a responsible leader in healthcare and result in employee sanctions (up to, and including, termination of employment), revocation of professional licensure/accreditation, significant civil monetary and/or criminal penalties. This standard applies to PSJH ePHI as well as, more broadly, to all PSJH information. Any references to particular regulatory or contractual requirements (e.g., HIPAA, FDA regulations, state laws, PCI-DSS) are intentionally minimized so as not to indicate that this policy is exclusive to specific categories of information (e.g., ePHI, PII, student records, employee records, genetic information, trade secret information).

Non-Compliance:

All PSJH workforce members shall understand their roles and responsibilities for protecting PSJH information and physical assets. Failure to comply with the Enterprise Information Security Policy may result in disciplinary actions up to and including termination of employment for employees or termination of contract for contractors, partners, consultants, and other entities. Violations may subject individuals (and the organization) to civil and/or criminal penalties.

References:

See the Social Media Policy, available on the HRPortal

PSJH-RIS-715 Records Retention and Disposal

Confidentiality Policy (available on the HRPortal)

PSJH-EIS-950.04 Vendor Security Risk Management

PSHJ-EIS-951.01 Information System Acquisition, Development and Maintenance

PSJH-EIS-951.02 Data Handling and Destruction

This document is classified PSJH Confidential. Do not redistribute without the approval of Risk & Integrity Services / Information Security Services.

Approval Signatures

Step Description	Approver	Date
PSJH President/CEO	Cynthia Johnston: Compliance Spec PSJH	05/2021
PSJH Executive Council	Cynthia Johnston: Compliance Spec PSJH	05/2021
PSJH Policy Advisory Committee	Cynthia Johnston: Compliance Spec PSJH	05/2021