HAWAII HEALTH SYSTEMS CORPORATION Quality Healthcare for All **PROCEDURE**	**Department:** **Information Technology Department (ITD)**	**Policy No.** **ITD 0051B**
		Supersedes Policy No. N/A
Subject: **Information Security**	**Approved By:** Linda Rosen By: Linda Rosen, M.D., M.P.H. Its: HHSC Corporate CEO	**Approved Date:** January 26, 2023
		Last Reviewed: December 20, 2022

I. PURPOSE:

To ensure the security of all information and provide guidelines to all Users to protect, monitor, and comply with federal and state laws and regulations. Provides direction and support for the management of information security in accordance with business requirements and relevant laws and regulations.

II. DEFINITIONS:

All capitalized terms not defined herein shall have the meaning set forth in the ITD Glossary. Applicable to all ITD policies and procedures.

III. PROCEDURE:

A. Information Security Standards

Information security documentation including, but not limited to, policies, standards, and procedures, shall be classified as “Internal Use Only,” unless expressly created for external business processes or partners.

Implementation of HHSC’s Information Systems security architecture shall be coordinated and managed by the HHSC IST. The IST is managed by the CISO, with oversight from the HHSC Audit and Compliance Committee.

HHSC requires that all systems adhere to the patch management strategies described in NIST SP 800-40r4 Guide to Enterprise Patch Management Planning Preventative Maintenance for Technology. Systems that are found to be non-compliant with HHSC policies may be censured from the network.

B. Systems Protection and Activity Monitoring

HHSC has the right to monitor individual User activity on its Information Assets, including computer systems, telephone systems, voice mail systems, internet activity, e-mail and other confidential information traffic at any time. Monitoring may be conducted on any basis, including routine, random or triggered by particular events or usage. Monitoring shall be conducted when there is evidence of any activity that is prohibited, violates HHSC policy, or might jeopardize the normal operation of the Information Assets. HHSC monitoring of individual communications may be reviewed and approved by HHSC Corporate and Regional Executive Leadership or its designee. Non-enforcement of any policy requirement does not constitute a waiver or consent by HHSC.

C. Policy Conflicts and Exceptions

HHSC Information Security policies are drafted to meet or exceed the protections found in existing laws and regulations. Any HHSC Information Security policy believed to be in conflict with existing laws or regulations shall be promptly reported to the CISO.

Unless expressly set forth, these policies are intended to supplement rather than supersede existing HHSC policies and procedures. In case of a conflict, the CISO shall be notified and shall work with the applicable Users to resolve the conflict.

Information Security Policy Exception Requests shall be submitted in writing by relevant Management to the CISO, who shall facilitate HHSC Corporate and Regional Executive Leadership review and approval. Requests shall include justification and benefits attributed to such exception. Exceptions to information security policies are permissible only in those instances where a risk assessment examining the implications of noncompliance has been performed and the CISO has approved and documented the exception.

D. Audit and Security Controls

HHSC Information Owners shall define a method of auditing their respective Information Systems to ensure compliance with the information classification policy (ITD 0009 Data Classification policy) and its guidelines. The ITD is responsible for developing an effective system to monitor access to the overall network, and to individual components as necessary. Periodic checks shall be made in all work areas to ensure that employees are aware of and complying with information security policies. All Information Systems security controls must be technically and operationally feasible and have a way to evaluate their alignment with existing security policies prior to being adopted as a part of standard operating procedures.

E. Security Education, Training and Awareness Requirements

All Users shall receive a copy of this policy and the HHSC Privacy and Security Handbook. This documentation will be provided to new Users during their initial orientation. Following initial orientation, Users shall complete information security awareness training as outlined in the table below. Additionally, HHSC Corporate and Regional Management shall orient new Users to any applicable Facility, HHSC Corporate Office or department-specific security procedures, and shall include information security and confidentiality in the annual performance review process for HHSC employees.

Users	Method and Frequency	Responsible Party
Physicians employed by HHSC, and Board Members	Initial orientation and periodic training.	New Employee Orientation and responsible manager
Physicians not directly employed by HHSC	Initial Confidentiality Acknowledgement and periodic renewal. Pre-education training as necessary for access to HHSC Information Assets.	Responsible Manager
Volunteers	Initial orientation, and periodic training, if appropriate.	Responsible Manager
Contractors	Initial orientation, and periodic training, if term is > 1 year.	Responsible Manager
Employees, Management, and ITD Staff	Initial orientation and periodic on-line training.	New Employee Orientation and responsible manager

F. Incident Reporting

All incident reports relating to information security shall be maintained by Corporate Compliance to assure the confidentiality of the document.

Users are responsible for:

- Using Information Assets for the purposes intended.
- Promoting awareness and use of applicable information security controls as defined by policies and procedures.
- Complying with custodian-established controls and backup procedures.
- Reporting the loss or misuse of Information Assets promptly to the CISO, Corporate Compliance and Privacy Officer, or their Manager.

G. Business Continuity Plan and Disaster Recovery

The impact analysis along with provisions for business continuity and risk assessment shall be updated periodically and kept on file with the IST. A Disaster Recovery Plan (DRP) shall be maintained on the HHSC Intranet by IST and HHSC Corporate and Regional Management under the oversight of the CISO. The DRP shall include provisions for continuity of Facility or department business operations and recovery in the event of disaster. Details for recovering critical information via backup and recovery operations shall be included in the DRP.

H. Review of Information Security Policy

The Information Security policy shall be reviewed periodically and when significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness. The review shall include feedback from relevant Users, with results of independent reviews and recommendations by management and relevant authorities. Changes in policy shall be in response to changes in the HHSC environment, business circumstances, legal conditions, or technical environment. A copy of the policy shall be maintained on the HHSC Intranet for easy access by Users.

The Privacy and Security Council is an appointed committee that recommends changes in policy, provides oversight for the program and approves exceptions to the HHSC Information Security policy. A cross section of HHSC personnel is assigned to this committee. The committee meets at least quarterly in conjunction with the Corporate Compliance Committee and is advisory to the HHSC Corporate and Regional Executive Leadership and HHSC Corporate Board of Directors. The CISO shall serve as the ITD information security staff contact for the committee. Refer to CMP 0021A Privacy and Security Council.

The CISO is responsible for all updates to the policy document. This document shall be reviewed and/or updated annually.

IV. REFERENCES:

- CMP 0021A Privacy and Security Council.
- ITD 0009 Date Classification policy.
- ITD 0051A Information Security policy.
- HHSC Privacy and Security Handbook.
- NIST SP 800-40r4 Guide to Enterprise Patch Management Planning Preventative Maintenance for Technology.