HAWAII HEALTH SYSTEMS CORPORATION *Quality Healthcare for All* **POLICY**	**Department:** **Information Technology Department (ITD)**	**Policy No.** **ITD 0051A** **Supersedes Policy No.** N/A
Subject: **Information Security**	**Approved By:** Stephany Vaioleti HHSC Board of Directors By: Stephany Vaioleti Its: Secretary/Treasurer	**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 and provide 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. POLICY:

A. Philosophy

Information is vital to Users to provide high quality patient care. HHSC utilizes information effectively, while protecting the information from unauthorized or inappropriate use. Data in all forms (electronic, paper, or other) throughout its life cycle (creation, storage, access, reproduction, transmission, distribution, and destruction) must be protected from unauthorized access, modification, disclosure, or destruction, whether accidental or intentional.

B. Information Security Standards

HHSC has adopted the National Institute of Standards and Technology (NIST) Standards for the management and implementation of information security. HHSC shall periodically review and update information security policies to ensure consistency with the NIST Standards and best practices. HHSC shall employ a policy-driven Information Systems security architecture approach that takes into consideration HHSC's business goals and objectives.

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 with a prioritization on mitigation and avoidance in risk management.

C. Protection and Use of Information

Each Information Asset shall be consistently protected in a manner commensurate with its sensitivity, value, and criticality. Information is a critical and vital asset, and all information shall be accessed, used, transmitted, reproduced, and stored in a manner that provides the maximum amount of protection from inappropriate disclosure while permitting efficient operation and professional conduct of HHSC business.

D. User Accountability and Responsibility

Each User shall follow this policy to protect information and to gain access to information needed to perform job duties or functions. Each User shall be aware of HHSC confidentiality and information security policies. If a User is assigned a logon ID and password for access to information, the User shall be responsible for maintaining the confidentiality of such information and shall not disclose the password to anyone. Refer to ITD 0113A User Responsibility policy and 0113B User Responsibility procedure.

E. Systems Protection and Activity Monitoring

HHSC uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by its computers and communications systems. In keeping with these objectives, HHSC maintains the authority to: (1) restrict or revoke any User's privileges, (2) inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives, and (3) take any other steps deemed necessary, up to and including disconnection of a compromised or non-compliant device from the HHSC network, to manage and protect its Information Systems. This authority may be exercised with or without notice to Users. HHSC shall not be responsible for loss or damage to data or Software that result from its efforts to comply with these security objectives.

No one shall willfully attempt to degrade the performance of or deny access to Information Assets, use loopholes in computer security systems or knowledge of a special password to damage Information Assets, obtain extra resources from another User, gain access to systems or accounts, or use systems or accounts for which proper authorization has not been granted. Violation by any User shall be cause for corrective action up to and including termination of employment in accordance with applicable collective bargaining agreements and may subject an individual to criminal prosecution or reporting to a licensing board or both.

F. Compliance with Legislative, Regulatory and Contractual Requirements

HHSC shall comply with the security requirements governing information as set forth in HIPAA, and other federal and state laws and regulations governing electronic security, as such may be amended from time to time. The HIPAA Administrative Information Security Standard sets forth the minimum requirements for compliance, and all Users are encouraged to exceed these minimal standards. All HHSC Information Owners and HHSC Corporate and Regional Managers shall review these laws and ensure that applicable standards are applied in their respective areas of responsibility. Users are advised that confirmed or suspected violations may be referred to law enforcement for investigation and prosecution.

G. Rights of Stakeholders

It is the policy of HHSC to respect and maintain the confidentiality of patients, business partners, Workforce, and Users. Refer to CMP 0019A, HIPAA Minimum Necessary policy.

H. Audit and Security Controls

Information Owners shall define a method of auditing their respective systems to ensure compliance with the Information Classification policy (ITD 0009 Data Classification policy) and its guidelines. ITD shall develop an effective system to monitor access to the overall network and to individual components as necessary.

I. Security Education, Training and Awareness Requirements

All Users permitted to access Information Assets shall be provided training on information security and their individual responsibilities regarding information security. All Users are hereby advised that HHSC Information Security policy and procedures are available on the HHSC Intranet.

J. Incident Reporting

All Users shall comply with the HHSC Information Security policy and report violations or suspected violations of this policy to their Manager or to the CISO or to the HHSC Corporate or Regional Compliance Officers and Privacy Officers.

K. Business Continuity and Disaster Recovery Management

Designated Information Owners shall assess the potential impact that loss of information would have on HHSC business activities.

L. Relationship to Existing Policies

These policies are intended to supplement rather than supersede existing HHSC policies and procedures unless expressly stated herein.

IV. RESPONSIBILITIES:

HHSC Corporate and Regional Executive Leadership shall be accountable for the operation of a successful, compliant information security program.

HHSC Corporate and Regional Management shall be accountable for the ownership of information and responsible for ensuring that adequate resources are in place for information security administration, including classification, criticality, access and disclosure, and risk analysis.

The HHSC IST shall work with HHSC Corporate and Regional Management on overall development, implementation, maintenance, and updating of information security policies and procedures, and provide support for information security in accordance with business requirements and relevant laws and regulations.

Information Owners, Business Owners, Security Contacts, and System Administrators implement, monitor and issue access codes, ensure access authorization, define access control profiles, monitor system security and integrity, and perform business continuity disaster recovery planning activities. The User Provisioning Team shall create unique user

ID's, establish one-time passwords that must be changed by the User at initial login, and grant the appropriate level of access to data per the request of the Responsible Manager.

Users shall preserve the confidentiality, integrity, and availability of information at the user level, comply with all information security standards and ITD policies, and report any security violations.

V. AUTHORITY:

- NIST SP 800-53 (Rev. 4).
- Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C; 45 CFR 164.310(b), 164.306.
- HIPAA.
- 45 C.F.R. 160 and 164, as amended.
- 45 CFR 164.308(a)(1)(i).

VI. RELATED PROCEDURE:

ITD 0051B.

VII. REFERENCES:

- CMP 0019A Minimum Necessary Standard Compliance policy.
- ITD 0009 Date Classification policy.
- ITD 0113A User Responsibilities policy.
- ITD 0113B User Responsibilities procedure.
- NIST SP 800-40r4 Guide to Enterprise Patch Management Planning Preventative Maintenance for Technology.