HAWAII HEALTH SYSTEMS CORPORATION *Quality Healthcare for All* **POLICY**	**Department:** **Information Technology Department (ITD)**	**Policy No.** **ITD 0026A**
		Supersedes Policy No. N/A
Subject: **Patch Management**	**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:

Establishes the requirement for applying software and firmware patches (collectively "Patch" or "Patches") and version upgrades as an integral component of the HHSC IT asset management program. Establishes cybersecurity vulnerability management as a critical sub-component of the overall asset management program. This policy ensures compliance with the HIPAA Security Rule requirements, and generally acknowledged IT best practices.

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:

Staff shall support Technical Services Division (TSD), Application Services Division (ASD), and Regional End-User Support Team (REST) System Administrators in tracking and managing upgrades and Patches to both applications and operating systems of devices in the HHSC infrastructure in accordance with the patch management strategies described in NIST SP 800-40r4 Guide to Enterprise Patch Management Planning Preventative Maintenance for Technology. Applying vendor-supported versions of applications and operating systems with current patches is critical to HHSC's cybersecurity and risk profiles. IT staff shall use various tools to detect and identify cybersecurity vulnerabilities in devices connected to the infrastructure. Patch Management Staff shall assign a Vulnerability Priority Rating (VPR) to guide remediation activities. TSD and REST System Administrators shall be responsible for installation of required Patches and upgrades identified by the ASD staff and the Patch Management Staff. Failure to remediate identified cybersecurity vulnerabilities may lead to censuring actions, including disconnecting the vulnerable device from the HHSC infrastructure.

This policy applies to Technical Services Department (TSD), Application Services Division (ASD), Regional End-User Support Team (REST), and the Patch Management Staff. For purposes of this policy, "Patch Management Staff" includes all staff with responsibility for ensuring stable and secure operations of the supported hardware and software through the application of Vendor provided patches and upgrades. Normally, the primary application support team will be the most knowledgeable of the specific patches required for the application software and the hardware platform upon which the application runs, and shall provide this information to the Patch Management Staff as part of the Configuration Management function.

IV. AUTHORITY:

- HIPAA.

V. RELATED PROCEDURE(S):

ITD 0026B.

VI. REFERENCE(S):

- NIST SP 800-40r4 Guide to Enterprise Patch Management Planning Preventative Maintenance for Technology.