

 <p><b>HAWAII HEALTH SYSTEMS</b> CORPORATION <i>"Touching Lives Everyday"</i></p> <p align="center"><b>Policy</b></p>	<b>Department:</b> Information Technology Department	<b>Policy No.:</b> <b>ITD 0026</b>
	<b>Issued by:</b> Barbara Kahana Vice President & CIO	<b>Revision No.:</b> N/A
<b>Subject:</b> <b>Security Patches</b>	<b>Approved by:</b>  Thomas M. Driskill, Jr. President & CEO	<b>Effective Date:</b> 10/04/04
		<b>Supersedes Policy:</b> N/A
		<b>Page:</b> Page 1 of 2

- I. **PURPOSE:** This policy establishes requirements for the application of security patches to IT systems. It is based on final HIPAA security rule requirements, and generally acknowledged IT best practices.
  
- II. **POLICY:** Security staff will support Technical Services Division (TSD), Application Services Division (ASD), and Regional End-User Support Team (REST) system administrators in identifying required security patches. TSD and REST system administrators will be responsible for installation of required security patches identified by the Security staff.
  
- III. **SCOPE:** This policy applies to Technical Services Division (TSD), Application Services Division (ASD), and the Regional End-User Support Team (REST).
  
- IV. **RESPONSIBILITIES**
  - A. **Security Staff Responsibilities**
    - Monitor security resources for newly released patches that are applicable to software used by HHSC.
    - Perform risk analyses to make recommendations regarding patch implementation.
    - Notify TSD and REST about required security patch installation requirements.
    - Coordinate with ASD to obtain vendor approvals for security patch installations.
    - Maintain patch activity log.
  
  - B. **ASD Responsibilities**
    - Upon notification of required security patches by the Security staff, ASD staff will contact application vendors to obtain verification that proposed patches are compatible with their software products.
    - Forward application vendor responses to the Security staff.

**C. TSD Responsibilities:**

- Upon notification of required security patches by the security staff, TSD staff will contact vendors of applications that are within the specific scope of responsibility to obtain verification that the proposed patches are compatible with their software products.
- Apply patches to systems under TSD jurisdiction.
- After Security staff provides notification that ASD software has been cleared by their respective vendors for patch installation, apply security patches.
- Verify proper installation of patches and forward notification of patch installation verification and completion to the Security staff.

**D. REST Responsibilities:**

- Upon recommendation of patch application by the security staff, REST staff will contact vendors of applications that are within the scope of responsibility of REST to obtain verification that proposed patches are compatible with their software products.
- Apply patches to those systems under REST jurisdiction.
- Apply patches to systems that host ASD controlled applications only after receiving notification from the security staff that application vendor approval has been obtained by ASD staff.
- Verify proper installation of patches and forward notification of patch verification and installation to the Security staff.
- Forward summary reports of end-user workstation patch installation verification status to the Security staff.