

 <p><b>HAWAII HEALTH SYSTEMS</b> CORPORATION <i>"Touching Lives Everyday"</i></p> <p><b>Policy</b></p>	<b>Department:</b> Information Technology Department	<b>Policy No.:</b> <b>ITD 0025</b>
	<b>Issued by:</b> Barbara Kahana Vice President & CIO	<b>Revision No.:</b> N/A
<b>Subject:</b> <b>Anti-Virus</b>	<b>Approved by:</b>  Thomas M. Driskill, Jr. President & CEO	<b>Effective Date:</b> 07/01/02
		<b>Supersedes Policy:</b> N/A
		<b>Page:</b> 1 of 2

- I. **PURPOSE:** This policy outlines criteria for protecting HHSC information assets from computer viruses.
- II. **POLICY:** This policy has been established in order to comply with Public Law 104-191, a federal law enacted on August 21, 1996, that is otherwise known as the Health Insurance Portability and Accountability Act (HIPAA).

Protection against computer viruses must be implemented throughout the entire HHSC information system. Virus protection must be installed at network perimeter gateway points, network servers, all desktop computers, and all portable computer devices that communicate with the HHSC network.

Procedures for monitoring and notification of virus alerts, and for the timely application of virus detection and cleaning updates will be developed and must be strictly adhered to.

Anti-virus responsibilities of IT staff who are responsible for configuring devices that communicate with the HHSC network include, but are not limited to the following:

- Installation and maintenance of anti-virus software on network perimeter gateway point devices, network servers, all desktop computers, and all portable computer devices.
- Ensuring that the most current anti-virus detection and remediation updates are applied.
- Promptly responding to notification of anti-virus detection and remediation updates by the HHSC Security staff.
- Notifying end-users of security alerts.

Anti-virus requirements for devices used to remotely access the HHSC computer system are specified in ITD 0006 - Remote Access Policy.

Responsibilities of the HHSC Security staff include, but are not limited to the following:

- Monitoring for virus alerts on a daily basis.
- Notifying IT staff of any emergency anti-virus detection and remediation updates.
- Alerting IT staff of significant virus outbreaks.

**III. SCOPE:** This policy applies to all IT staff and Security staff.

**IV. RESPONSIBILITIES:** The IT staff and Security staff shall be responsible for implementing this policy.

**V. REFERENCES/RELATED POLICIES**

- ITD 0002 – Security Configuration Management
- ITD 0006 – Remote Access

**VI. POLICY DEVELOPMENT**

DEVELOPER: Taylor Summers  
Miles Sato, CISSP