HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Information Technology Department	Policy No.: **ITD 0006**
		Revision No.: 1
Policy	Issued by: Barbara Kahana Vice President & CIO	Effective Date: 10/04/04
Subject: ***Remote Access***	Approved by: Thomas M. Driskill, Jr. President & CEO	Supersedes Policy: 03/01/02
		Page: Page 1 of 2

I. **PURPOSE:** This policy establishes security requirements for eligible employees, physicians, and vendors who require remote electronic access to HHSC information systems. It is based on external auditor recommendations, final HIPAA security rule requirements, and generally acknowledged IT best practices.

II. **POLICY:** The following Security requirements for eligible employees, physicians, and vendors who require remote electronic access to HHSC information systems will be adhered to:

A. User Access Control: Access to HHSC information systems from remote locations must be approved by the User's department manager. Non-HHSC employees must establish contractual agreements with HHSC in compliance with State and federal laws. Access lists of all entities granted remote access privileges will be subject to periodic review to confirm continuing appropriateness of remote access privileges.

B. Vendor Restrictions: Vendors who are contractually required to remotely access HHSC systems for maintenance purposes shall be allowed such access, subject to the provisions set forth in this policy.

C. Approved Access Methods:

1. **Telephone Access Configuration Control:** Telephone line dial-up modem access will only be allowed through (a) the HHSC secure modem pool, or (b) through specially configured modems for select vendors to use for the duration of their contractually required maintenance activity. Specially configured vendor access modems must not allow any dial-in access, except during contractually pre-arranged vendor maintenance work times. Dial-in access to these vendor accessible modems will be strictly controlled by HHSC IT staff.

2. **Internet-Based Access Configuration Controls for Users:** Internet-based access into HHSC's internal network by specified Users is allowed only by means of Virtual Private Network (VPN) technology with encryption enabled.

Encryption must conform to current National Institute of Standards and Technology (NIST) encryption standards.

3. **Internet-Based Access Configuration Controls for Vendor Support:** Internet-based access into HHSC's internal network by Vendors who need to provide remote support functions on their products is allowed by means of either Virtual Private Network (VPN) technology, as is described above, or by approved web-based remote-control support mechanisms.

B. Logging Requirements: Logs of inbound remote access activity must be maintained and periodically reviewed. Log review procedures shall be developed to comply with periodic log review requirements.

C. Remote Workstation Hardware Configuration: If hardware to be used for remote access purposes is supplied and owned by HHSC, the following configuration controls must be implemented on remote access workstations (whether desktop PC based or portable notebook computer based). Documentation attesting to conformance with the following implementation requirements must be kept on file:

1. Anti-virus software must be installed, and virus signature files must be kept up to date.

2. A personal firewall product must be installed and properly configured.

The personal firewall requirement is not a standard internal HHSC workstation configuration requirement.

If hardware to be used for remote access purposes is not supplied by, or owned by HHSC, the above hardware configuration specifications must be strongly recommended, unless specified by contractual arrangement.

III. SCOPE: This policy applies to all HHSC employees, volunteers, trainees, physicians and healthcare providers, independent contractors, vendors, and any other persons whose conduct in the performance of work for HHSC is under the direct control of HHSC, whether or not they are paid by HHSC.

IV. DEFINITIONS:

- **Independent Contractor:** an individual or legal entity who provides services to HHSC.
- **Personal Firewall Product**: refers to either a software-based firewall product installed on a remote workstation, or a hardware-based firewall product connected to a remote workstation.
- **Vendor:** any entity, including, but not limited to any individual that provides goods and/or services to HHSC.

V. REFERENCES/RELATED POLICIES:

- ITD 0005 - Information Systems Access Policy