

 <p>HAWAII HEALTH SYSTEMS C O R P O R A T I O N "Touching Lives Everyday"</p> <p>Policy</p>	Department: Information Technology Department	Policy No.: ITD 0005
	Issued by: Barbara Kahana Vice President & CIO	Revision No.: 1
Subject: Information Systems Access	Approved by: Thomas M. Driskill, Jr. President & CEO	Effective Date: 10/04/04
		Supersedes Policy: 03/01/02
		Page: 1 of 2

- I. **PURPOSE:** This policy mandates adequate levels of security to protect HHSC data and information systems from unauthorized access. The rules necessary to achieve this protection and to ensure a secure and reliable operation of HHSC information systems are defined in this policy. This policy is based on external auditor recommendations, final HIPAA security rule requirements, and generally acknowledged IT best practices.
- II. **POLICY:** Only authorized users shall be granted access to information systems, and users are limited to specific defined, documented and approved applications and levels of access rights. Department managers are responsible for granting user access authorization. Computer and communication system access control is achieved via user IDs that are unique to each individual user to provide individual accountability.

Access Control: Any User (remote or internal), accessing HHSC networks and systems, will be granted access to information based on:

1. Context-based criteria (access based on the context of a transaction)
2. Role-based criteria (access based on predefined roles)
3. User-based criteria (access based on the identity of a user)

Workstation Access Control: All workstations must use HHSC approved access control systems. Access must be restricted on all active workstations left unattended for prolonged periods of time.

Disclosure Notice: Where feasible a warning notice will be displayed when logging on to HHSC systems. The warning notice will make it clear that these systems are part of a private network or application, and unauthorized users should disconnect or log off immediately.

Access Control Mechanisms: Access control mechanisms must be utilized to ensure that information is not improperly disclosed, modified, deleted, or rendered unavailable.

Data Access Approval: Access to information stored on information systems will not be granted to any user without appropriate department manager approval.

Access for Non-Employees: Non-workforce members (i.e. independent contractors and vendors) are required to enter into a partnership agreement with HHSC in compliance with State and federal laws. Department managers must approve non-employee access.

Unauthorized Access: Users are prohibited from attempting to gain access to any information system, application, or data outside the scope of their work duties.

Remote Access: Security requirements for remote access to HHSC information systems are documented in the Remote Access Policy (ITD 0006).

Emergency Access: Procedures shall be implemented for obtaining access to necessary information during an emergency.

Maintenance/Helpdesk Remote Control Access: Procedures may be implemented for IT staff to remotely access user workstations for maintenance/helpdesk purposes. Remote control access to users workstations by IT staff must be given prior approval by the user. Exceptions to user access requirements may be granted by department managers for emergency situations. Logs of all remote control access sessions to user workstations must be recorded and maintained.

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.
- **User:** is any person or entity that accesses HHSC data and information systems. Users include healthcare providers, independent contractors, physicians, vendors, and workforce members.
- **Vendor:** is any entity, including, but not limited to any individual that provides goods and/or services to HHSC.
- **Workforce:** includes employees, volunteers, trainees, and 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.

V. REFERENCES/RELATED POLICIES

- ITD 0006 - Remote Access Policy