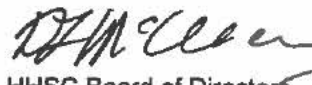
 HAWAII HEALTH SYSTEMS CORPORATION <i>Quality Healthcare for All</i> POLICY	Department: Information Technology Department (ITD)	Policy No. ITD 0005A
		Supersedes Policy No. N/A
Subject: Information Systems Access	Approved By:  HHSC Board of Directors By: Donna McCleary, M.D. Its: Secretary/Treasurer	Approved Date: January 23, 2020
		Last Reviewed: 01/21/20

I. PURPOSE:

To mandate adequate levels of information technology security to protect HHSC data and Information Systems from unauthorized access by defining the rules necessary to protect and secure the reliable operation of HHSC Information Systems.

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:

Only authorized Users shall be granted access to Information Systems. Access shall be limited to specifically defined, documented approved applications, and approved levels of access rights. Department managers are responsible for requesting User access.

Authorization shall be documented on an IT Security Access Request Form. Computer and communication system access control is achieved via User ID's that are unique to each individual User to provide individual accountability. Users are prohibited from sharing passwords with anyone, including IT personnel. Failure to comply with ITD policies and procedures shall result in loss of Information System access privileges and may include disciplinary action upon completion of a thorough investigation. Any disciplinary action shall be conducted in accordance with applicable collective bargaining unit agreements, if any, and with HR Guidelines.

A. Access Control

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

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

B. Workstation Access Control

All Workstations shall utilize HHSC-approved access control systems. Active Workstations left unattended for longer than five minutes shall be locked, logged off, or powered down.

C. Disclosure Notice

Where feasible, a warning notice shall be displayed when logging on to HHSC Information Systems. The warning notice shall make clear that these Information Systems are part of a private network or application, and that unauthorized Users should disconnect or log off immediately.

D. Access Control Mechanisms

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

E. Data Access Approval

Access to information stored on Information Systems shall not be granted to any User without appropriate department manager approval evidenced by a completed HHSC Corporate IT Security Access Request Form.

F. Access for Non-Workforce Members

Non-Workforce members (i.e., Independent Contractors and Vendors) shall be required to enter into a Business Associate Addendum with HHSC in compliance with state and federal laws. Department managers shall approve non-Workforce member access by completing the ITD Security Access Request Form and submitting it to the Regional Compliance Officer or Regional CEO and IST.

G. Unauthorized Access

Users are prohibited from attempting to gain access to any Information Systems, application, or data outside the scope of their work duties or level of access.

H. Remote Access

All eligible Workforce, physicians, Independent Contractors, and Vendors who require remote electronic access to HHSC Information Systems shall comply with the following security requirements:

1. User Access Control

- a. Access to HHSC information systems from remote locations shall be approved by the User's department manager via the IT Security Access Request Form, which shall be submitted to the Regional Compliance Officer and IST for approval. Non-Workforce members shall not have remote access unless HHSC has executed a written agreement permitting such access. A master access list, maintained by the ITD, of all persons granted remote access privileges shall be subject to periodic review to determine the appropriateness of continued remote access privileges.

2. Vendor Restrictions

- a. Vendors who are contractually required to remotely access HHSC Information Systems for maintenance purposes shall be allowed such access, subject to the provisions set forth in this policy.

3. Approved Access Methods

- a. **Internet-Based Access Configuration Controls for Users:** Internet-based access into HHSC's internal network by eligible remote Users is allowed only by means of VPN and Virtual Desktop technology with encryption enabled. Encryption shall conform to current National Institute of Standards and Technology (NIST) encryption standards.
- b. **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 are allowed by means of either VPN Virtual Desktop technology, as is described above, or by approved web-based remote-control support mechanisms.

4. Logging Requirements

- a. Logs of inbound remote access activity shall be maintained and periodically reviewed by System Administrators. Log review procedures shall be developed to comply with periodic log review requirements.

5. Remote Workstation Hardware Configuration

- a. If hardware to be used for remote access purposes is supplied and owned by HHSC, the configuration controls listed below shall be implemented on remote access devices. Documentation attesting to conformance shall be maintained in the ITD files:
 1. Anti-virus software shall be installed, and virus signature files shall be kept up to date.
 2. A personal firewall product shall be installed and properly configured. The personal firewall requirement is not a standard internal HHSC Workstation configuration requirement.
- b. If hardware to be used for remote access purposes is not supplied by, or owned by HHSC, the above-referenced hardware configuration specifications are strongly recommended, unless otherwise specified by contract.

I. Emergency Access

ITD shall create and implement procedures for obtaining access to necessary information during an emergency.

J. Maintenance/Helpdesk Remote Control Access

ITD may remotely access User Workstations for maintenance/helpdesk purposes.

IV. AUTHORITY:

- HIPAA [45 CFR §164.308(a)(3)(ii)(A)] [NIST SP 800-53 AC-1] [NIST SP 800-53 AC-3] [NIST SP 800-53 MP-2].
- NIST Special Publication 800-124 Revision 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise.

V. RELATED PROCEDURE:

None.

VI. REFERENCES:

- Security Access Request Form.