

 <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 0012</b>
	<b>Issued by:</b> Barbara Kahana Vice President & CIO	<b>Revision No.:</b> 1
<b>Subject:</b> <b>Password</b>	<b>Approved by:</b>  Thomas M. Driskill, Jr. President & CEO	<b>Effective Date:</b> 10/04/04
		<b>Supersedes Policy:</b> 07/01/02
		<b>Page:</b> 1 of 2

- I. PURPOSE:** This policy establishes password creation and usage criteria for user derived passwords. The HHSC Information Systems Access Policy (ITD 0005) requires that systems access be controlled by means of user IDs that are unique to each individual user. An approved means for authenticating individual users will be the use of passwords.

It is understood that passwords are inherently easily compromised, and that their strength is highly dependent on their difficulty in being guessed, and on how well they are protected.

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).

- II. POLICY:** The following criteria must be followed by Users of all HHSC information systems to protect the security and integrity of these assets.

User created passwords must be relatively difficult to be guessed, and must be properly protected because users will be held responsible for all actions undertaken with their personal user IDs. The following criteria must be followed when creating and using passwords:

- Passwords must not be shared or revealed to anyone besides the authorized user.
- Passwords must not be written down and left where unauthorized individuals might discover them.
- Newly created user accounts will use a unique temporary password supplied by the system administrator, which must be changed after the first successful logon.
- User created passwords must contain at least seven (7) characters.
- No more than five (5) consecutive unsuccessful logon attempts will be allowed. After the fifth unsuccessful logon attempt, an account must be temporarily disabled for no less than 15 minutes.

- All user created NT domain and AS/400 passwords must be changed every 90 days or less.

**III. SCOPE:** This policy applies to all HHSC employees, volunteers, trainees, physicians and healthcare providers, independent contractors, vendors, and any other persons under the direct control of HHSC.

**IV. RESPONSIBILITIES:** Every user of information systems must comply with the provisions stated in this document.

**V. REFERENCES/RELATED POLICIES**

- ITD 0005 - Information Systems Access Policy