HAWAII HEALTH SYSTEMS CORPORATION "Touching Lives Everyday"	Department: Information Technology Department	Policy No.: **ITD 0015**
		Revision No.: N/A
Policy	Issued by: Barbara Kahana Vice President & CIO	Effective Date: 09/01/02
Subject: ***Information Risk Management***	Approved by:	Supersedes Policy: N/A
	Thomas M. Driskill, Jr. President & CEO	Page: 1 of 2

I. PURPOSE: Information risk management is the process of identifying HHSC information assets and the potential security threats to which these assets may be vulnerable. Appropriate controls must then be instituted into the business processes associated with these information assets to reduce information risk, while not significantly impeding the business processes. Information risk is defined to be the probability that a threat source will exploit or trigger a system vulnerability, and the subsequent potential for harm or loss of HHSC information assets that can result from the exploitation or triggering of a system vulnerability. This policy addresses requirements for reducing the likelihood of risk to HHSC information assets.

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).

The following shall be implemented to reduce information risk:

- The security staff will perform an information risk assessment analysis on all information assets. This analysis will identify likely threats and vulnerabilities to these information assets.
- The security staff will develop and implement risk management procedures to reduce risks to information assets, and will continuously monitor these procedures to evaluate their effectiveness.
- In compliance with the Security Awareness Training Policy (ITD0014), the security staff will oversee the development of user awareness and training activities in order to ensure user understanding of policies and procedures, which are designed to reduce risk.

III. RESPONSIBILITIES: The Corporate Information Security Officer (CISO), under the direction of the Corporate Information Officer (CIO) shall be responsible for managing information risk management activities of the security staff.

IV. REFERENCES/RELATED POLICIES

- ITD 0014 - Security Awareness Training
- GAO/AIMD-98-68, Information Security Management, May 1998

V. POLICY DEVELOPMENT

DEVELOPER: HRC Policy Committee
Taylor Summers
Miles Sato, CISSP