

 <p>HAWAII HEALTH SYSTEMS C O R P O R A T I O N <i>"Touching Lives Everyday"</i></p> <p>Policy</p>	Department: Information Technology Department	Policy No.: ITD 0021
	Issued by: Barbara Kahana Vice President & CIO	Revision No.: N/A
Subject: <i>Business Continuity/ Disaster Recovery Plans</i>	Approved by: Thomas M. Driskill, Jr. President & CEO	Effective Date: 09/01/02
		Supersedes Policy: N/A
		Page: 1 of 2

- I. **PURPOSE:** Continuity of critical information technology (IT) services must be ensured throughout HHSC. In the event of a major disaster essential IT services must be restored within a reasonable amount of time, and recovery efforts should begin soon afterwards.
- 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 security staff will coordinate the efforts of all business units of HHSC to develop a Business Continuity Plan (BCP) to ensure continuity of critical IT services. This plan must take into account all critical business functions supported by these services. It must be designed to minimize the risk and duration of disruption to HHSC business processes, in the event of damage to, failure of, loss of, or corruption of the IT infrastructure.

The security staff will also coordinate the efforts of information technology (IT) units within the Information Technology Department (ITD) to develop a corporate-wide IT Disaster Recovery Plan (DRP) to ensure proper responses to emergencies, and in the event of a disaster, to ensure the timely and efficient post-disaster recovery of damaged IT systems.

The safety, health, and well-being of the workforce shall be given priority consideration during the formulation of these plans.

The security staff will maintain and test both the BCP and DRP on a regular basis. At a minimum, they must be tested at least annually. Modifications to correct any discrepancies that arise as the result of these tests will be overseen by the security staff. Key personnel as defined within the plans must also be adequately and regularly trained with respect to their specific duties as are specified in the plans.

III. SCOPE: This policy applies to all critical business processes supported by the HHSC IT infrastructure.

IV. RESPONSIBILITIES: The Corporate Information Security Officer (CISO), under the direction of the Chief Information Officer (CIO) shall be responsible for managing the implementation of the BCP and DRP. It is understood that the development, implementation, maintenance, and training efforts will require the participation of all business units within HHSC.

V. POLICY DEVELOPMENT

DEVELOPER: Taylor Summers
Miles Sato, CISSP