

 <p><b>HAWAII HEALTH SYSTEMS</b> C O R P O R A T I O N "Touching Lives Everyday"</p> <p><b>Policy</b></p>	<b>Department:</b> Information Technology Department	<b>Policy No.:</b> <b>ITD 0027</b>
	<b>Issued by:</b> Barbara Kahana Vice President & CIO	<b>Revision No.:</b> N/A
<b>Subject:</b> <b>Contingency Plan</b>	<b>Approved by:</b>  Thomas M. Driskill, Jr. President & CEO	<b>Effective Date:</b> 10/04/04
		<b>Supersedes Policy:</b> N/A
		<b>Page:</b> 1 of 4

I. **PURPOSE:** This policy defines the requirements for development of a contingency plan to respond to information system emergencies. This plan will ensure that information required for mission-critical and essential business operations will remain available for use in the event of a major emergency such as a natural disaster, act of terrorism, or system failure that disrupts normal business operations. This contingency plan shall support the more encompassing Business Continuity Plan.

## II. POLICY

### A. Plan Components

An information systems contingency plan shall be established and maintained. This plan shall include specifications and documentation for identifying critical information systems and data, for ensuring up-to-date backups of systems and data, for specifying the organization and processes to be followed to respond and recover from an emergency, and for ensuring its ongoing testing and revision. The basic requirements for each component of the plan are:

1. Systems And Data Criticality Analysis – critical and essential information systems and data that high priority business operations depend on shall be identified and classified. An assessment of the vulnerabilities of such critical and essential systems and data shall also be performed, relative to various types of emergencies. Controls needed to prevent or minimize the effects of potential loss must be described. Documentation should include:
  - a. A cross-reference between business functions and information systems (applications and technologies)
  - b. A risk analysis identifying potential events that could cause key information systems to fail.
  - c. An impact analysis indicating the consequences of disruption to various business functions, taking into consideration:

- 1) Duration of the disruption
  - 2) Timing relative to business cycles (month-end, quarter-end, year-end, etc.)
- d. A clear statement of risk assumptions with definitions of minimum acceptable levels of service in business functions
  - e. Prioritization of information systems into categories of criticality.
  - f. Action plans to prevent and minimize risk of business interruption.
2. Systems and Data Backup and Recovery Plan – document and regularly update procedures for creating, maintaining, and retrieving exact copies of information, for specified periods of time. Also document how backup systems and/or facilities will be provisioned to make stored information accessible during an emergency. Documentation should include:
- a. The data backup schedule for every critical and essential information system
  - b. Data recovery procedures for every critical and essential information system
  - c. Specifications of the required data recovery systems and facilities (backup media, software, hardware, infrastructure, locations).
  - d. Plans for handling unsaved work in progress
3. A Disaster Recovery Plan - document the systems, resources, roles, responsibilities, and processes that will enable HHSC to restore any loss of data in the event of system emergency, and to restore critical and essential system functions. Indicate the recovery priorities of required systems, as well as their interdependencies, so that recovery sequences can be anticipated. This recovery plan relies on the documentation of the two preceding plan components, and adds the following additional components:
- a. A disaster recovery organization chart with functional descriptions
  - b. Staffing assignments (including alternate staffing.)
  - c. Emergency contacts
  - d. Recovery action plan, identifying key contingencies and the specific recovery procedures to be followed given each contingent factor
  - e. Quality checks for recovered systems
  - f. Startup, transition to return and shutdown of any alternative facility
  - g. Basic workstation recovery procedures

4. Emergency Mode Operation Plan - document the necessary systems, resources, roles, responsibilities, and processes that will enable HHSC to continue to operate during the time of a system emergency. This plan will complement the disaster recovery plan by specifying how HHSC will be mobilized to carry-on until systems are restored and normal business operations can be resumed. Documentation should include:
  - a. An emergency assessment and notification process that defines how different emergencies will be detected, assessed as to criticality, and communicated to appropriate personnel
  - b. Identification of emergency roles and responsibilities. Identify key authorities who will:
    - 1) assess and declare an emergency status
    - 2) mobilize staff
    - 3) manage emergency mode operations
    - 4) keep the public informed
  - c. Downtime and work-around procedures for all critical business functions
  - d. Downtime and work-around procedures for the interfaces between critical business functions
5. Testing And Revision Procedures - to discover and remedy weaknesses in the contingency plan, document procedures to periodically test each part of the plan, and to subsequently revise the documentation, as necessary. Pre- and follow-up training of all personnel who have a role in carrying out the contingency plan must also be addressed.

Depending on whether an information system has department-specific, multi-department or organization-wide applicability, each component of the systems contingency plan may have departmental as well as organization-wide provisions. Department-specific plans will be developed and maintained by the appropriate departments and incorporated into the overall HHSC contingency plan.

#### B. Contingency Planning Roles and Responsibilities

Each component of the information systems contingency plan shall include specific organizational roles and responsibilities relative to the objectives and scope of that component – e.g., the Emergency Mode Operation Plan will define the roles and responsibilities of various positions necessary to continue operations during an emergency. Described below are the roles and responsibilities required for development and maintenance of the information systems contingency plan:

1. Senior Management – Approves this policy; empowers the Contingency Planning Officer and Contingency Planning Committee, and approves and enforces the information systems contingency plan.
2. Contingency Planning Officer (could be the Information Security Officer) – Serves as liaison to Senior Management; chairs the Contingency Planning Committee, leads the development of analyses and plans, leads the testing and revision of contingency plans, and coordinates department participation and education.
3. Contingency Planning Committee – Represents critical operational areas of the organization, plus Information Systems, Telecommunications, Public Relations, Physical Plant, Security and Finance departments; serves as work group in the development of the contingency plan; participates in the execution of testing and review procedures, reviews and makes recommendations on department contingency plans.
4. Department Managers – Participate in and become knowledgeable about the Corporate contingency plan; organize department teams, develop and implement department plans, and provide training for staff.
5. Staff – Receives training, carries out specific tasks per the contingency plan.

### III. DEFINITIONS

System Emergency - A major information system failure or disaster, whether caused by equipment failure, natural disaster, accident or deliberate action, that threatens the disruption of critical and essential business processes.

Critical Business Operation – A crucial function of the organization whose disruption could have major detrimental impact on the organization if not restored within \_\_\_\_ hours. In a healthcare provider organization, for examples, critical business functions include obtaining patient charts and diagnostic test results during the delivery of patient care.

Essential Business Operation – A vital function of the organization whose disruption could have serious consequences if not fixed within \_\_\_\_ day(s) of the outage. In a healthcare organization, for example, essential business functions include the sending of claims and receiving of payments for the revenue on which the organization depends.