	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 6.1.0</b>
	<b>Title: CONTINGENCY PLANNING STANDARD</b>	<b>Page: 1 of 3</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/09/01</b>

**Contingency Planning Standard**

**I. SCOPE**

This standard applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This standard applies to all Tenet divisions, facilities, and related departments.

**II. PURPOSE**

Define roles and responsibilities for implementing a Contingency Planning program throughout Tenet facilities that provides a standard application of program principles while supporting flexibility of implementation at each facility. As authorized by management, the Contingency Planning Standard defines disaster criteria for the facility and defines responsibilities of program administrators.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception will be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.


**III. STANDARD**

The following standards shall be agreed-upon and approved by facility management:

- a) A Contingency Planning Program budget shall be allocated to support plan development and maintenance;
- b) A “Key Disaster Scenario” shall be defined by each facility and used as the basis to design, develop, activate and execute the Contingency Plan (“CP”); and
- c) Contingency Planning Program administrators shall be entrusted with the responsibility to develop, implement, maintain, test and execute a Data Criticality Analysis, Data Backup Plan, Business Continuity Plan, Emergency Response Plan, and Disaster Recovery Plan.

A. Key Disaster Scenario

The Key Disaster Scenario shall be used as the basis to design and develop the Contingency Plan. The Key Disaster Scenario represents the worst-case conditions of a disaster, which:

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 6.1.0</b>
	<b>Title:</b> <b>CONTINGENCY PLANNING STANDARD</b>	<b>Page: 2 of 3</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/09/01</b>

- a) Is severe in magnitude;
- b) Occurs at the worst possible time;
- c) Inflicts majority loss of critical resources to conduct business; and
- d) Requires implementation of the CP.

**B. Budget Requirements**


The principal budget requirements are for labor, supplies and services to fulfill component obligations of the Contingency Planning Program; specifically to develop and implement the:

- a) Data Criticality Analysis (“DCA”);
- b) Data Backup Plan (“DBP”);
- c) Business Continuity Plan (“BCP”), Emergency Response Plan (“ERP”) and Disaster Recovery Plan (“DRP”);
- d) Contingency testing plan, including testing for the BCP, ERP and DRP;
- e) Recovery plan maintenance of the BCP, ERP and DRP;
- f) Disaster training and awareness program; and
- g) Other potential network, hardware and software in support of the Contingency Planning Program.

**C. Emergency Response Team (ERT)**

The ERT is the key disaster recovery team and is activated in the initial phase of an emergency. The ERT’s primary roles during a disaster include:

- a) Ensuring the safety of individuals;
- b) Providing initial response review;
- c) Making decisions regarding the level of disaster response;
- d) Planning, coordinating, exercising, managing and maintaining the Contingency

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 6.1.0</b>
	<b>Title:</b> <b>CONTINGENCY PLANNING STANDARD</b>	<b>Page: 3 of 3</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/09/01</b>

Plan; and

- e) Coordinating plan development, response and recovery with all department managers.

Prior to an emergency, the ERT shall approve the recovery resources and procedures documented in the BCP, ERP and DRP. The ERT shall include management from the following areas:

- a) Administration (CEO, COO) – Chairperson;
- b) Security Officer;
- c) Information Systems;
- d) Law or Compliance;
- e) Facility Security;
- f) Human Resources;
- g) Accounting (CFO); and
- h) Public Relations.

#### **IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following documents:

- Contingency Planning Policy No. 6.0.0.
- Contingency Planning Procedure No. 6.1.1.
- Asset Access Control Standard No. 8.1.0.
- Backup Procedure No. 8.2.3.