	Information Security Policies and Procedures	No. COMP-Sec 8.2.3
	Title: BACKUP PROCEDURE	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 01/17/01

Backup Procedure

I. SCOPE

This procedure 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 procedure applies to all Tenet information assets and information asset Administrators.

II. PURPOSE

Provide direction for Tenet information asset Administrators regarding required backup procedures. Backup of Tenet information assets is a critical element in protecting the integrity, confidentiality, and availability of those assets.

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

III. PROCEDURE


Department managers or their delegates shall ensure that backups of critical data are made. Critical data should not be resident on microcomputers (PC), workstations, or small systems. However, where this is unavoidable, these systems shall be included in the backup plan.

A. Backup Requirements

Tenet information assets shall be backed up and the back up information stored to ensure recoverability. The frequency and handling of backups is directly affected by the criticality of the information, the difficulty in recreating the information and regulatory mandates. See the Contingency Planning Policy No. 6.0.0 and its associated Standard and Procedures, especially the sample Data Criticality Analysis in Addendum B to the Contingency Planning Procedure No. 6.1.1, for further information on categorizing the criticality of information assets.

B. Backup Administration

The facility’s backup administration procedures shall be documented in its Data Backup Plan in accordance with the Contingency Planning Procedure No. 6.1.1. Administrators of information assets shall back up files using the following guidelines:

	Information Security Policies and Procedures	No. COMP-Sec 8.2.3
	Title: BACKUP PROCEDURE	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 01/17/01

1. BACKUP GENERATION


Backups should be generated for all systems that maintain data critical to the facility. Backups should include all systems identified as Categories 1-4 in the facility's data criticality analysis. Backup planning should be conducted for all critical systems, and should include a backup schedule for each system.

- a) The following is a recommended backup schedule for most file servers:
 - (i) An incremental or differential backup shall be performed Monday through Sunday. This is a DAILY backup and shall be retained for two (2) weeks.
 - (ii) A full backup shall be performed once per week. This is a WEEKLY backup and shall be retained for four (4) weeks.
 - (iii) Shall an archival backup be needed, select a particular point in the month (first or last full backup, etc). Designate this as a MONTHLY backup and retain according to the Corporate Records Retention Policy.
- b) The following is a required backup schedule for all mail servers:
 - (i) Full backups will be performed daily, seven days per week.
 - (ii) Backups will be taken off-site and retained for thirty (30) days before being re-used.

2. BACKUP STORAGE

Backups shall be stored off site. Preferably, the backups will be stored at a different physical campus, but storage in a separate building from the primary server is also acceptable. If some backup tapes are stored on site, they shall be stored in a secure location such as a tape library with appropriate safeguards or a safe rated for computer media.


- a) Tape labels, whether electronic or hard copy, shall contain the following information:
 - (i) Facility;

	Information Security Policies and Procedures	No. COMP-Sec 8.2.3
	Title: BACKUP PROCEDURE	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 01/17/01

- (ii) System name;
 - (iii) Creation date;
 - (iv) Expiration date;
 - (v) Contents; and
 - (vi) Number of tapes in the set (1 of, 2 of).
- b) Backups shall remain off site until they are ready to be reused.
 - c) Data stored on computer media for a prolonged period shall be tested periodically to ensure that the information is recoverable.
 - d) Second copies of the backup may be stored on site in a tape library or secured vault.
 - e) A log of all backup media shall be maintained by those responsible for sending media off site for storage. A copy of the log shall also be maintained in an off-site, central location. The log shall include:
 - (i) Creation date;
 - (ii) Expiration date; and
 - (iii) Shipping container number for off-site storage.
 - f) A Business Associate Agreement (BAA) shall be executed with backup storage vendors.
3. BACKUP RETENTION

Backups are retained for two primary purposes, record retention and data restoration. If a backup is being retained for more than one purpose, then it shall be retained for the longer of the two required periods of time.

- a) Backups retained for the purpose of record retention shall be retained according to Tenet's Records Management Policy.

	Information Security Policies and Procedures	No. COMP-Sec 8.2.3
	Title: BACKUP PROCEDURE	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 01/17/01

- (i) See Information Security Awareness Training Standard No. 3.2.0.
 - (ii) See the Human Resources Policies & Procedures No. 306 “Records Retention” for further information.
 - (iii) See the Corporate Record Retention Schedule for other possible retention requirements.
- b) Backups retained for the purpose of restoring data shall be retained for a period of time sufficient to allow for an adequate backup tape rotation.

4. BACKUP RETRIEVAL


Backups shall be accessible in time to allow for system restoration within the required period of time for that system. If necessary, the ability to ship the tapes to remote sites for Disaster Recovery should be considered. The backup retrieval requirements, by data criticality category, are as follows:

- a) Category 4: Backups shall be retained at hot site in redundant system.
- b) Category 3: Backups shall be accessible in time to allow for system restoration within 24 hours.
- c) Category 2: Backups shall be accessible in time to allow for system restoration within 72 hours.
- d) Category 1: Backups shall be accessible in time to allow for system restoration within a reasonable amount of time (longer than 72 hours).
- e) Category 0: No backup requirements.

5. BACKUPS OF NETWORK ASSETS

Changes and updates to network assets (configuration, ACLs, etc.) shall be backed up.

- a) The target of the backup shall be a server designated by the Network Administrator.
- b) This server shall be backed up according to these procedures.

	Information Security Policies and Procedures	No. COMP-Sec 8.2.3
	Title: BACKUP PROCEDURE	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 01/17/01

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0 and its subordinate Standard and Procedure.
- Information Access Control Standard No. 3.1.0.
- Contingency Planning Policy No. 6.0.0 and its subordinate Standard and Procedure.
- Security Risk Management Standard No. 7.1.0.
- Technical Security Administration Policy No. 8.0.0.
- Logging and Auditing Procedure No. 8.2.2.
- Network Security Administration Standard No. 8.3.0 and its subordinate procedures.
- Operating System Security Standard No. 8.4.0.
- Application Security Administration Standard No. 8.5.0.
- Tenet Human Resources Policies and Procedures No. 306 “Records Retention”.
- Tenet Corporate Record Retention Schedule.
- Tenet Facility Security Plan.