	Information Security Policies and Procedures	No. COMP-Sec 5.1.0
	Title: INFORMATION ASSET SECURED AREA PROTECTION STANDARD	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 11/03/00

Information Asset Secured Area Protection 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 members of the Tenet Workforce.

II. PURPOSE

Provide guidelines regarding the use and protection of data centers, wiring closets and other secure areas that house, support, and protect Tenet Information Assets. Tenet information assets shall be located in rooms or areas that can be secured from loss or damage due to natural or manmade events.

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

All information assets such as mainframe or midrange computers, servers, network routers, switches, communication equipment and other critical assets shall reside in a secured and controlled environment.

- a) All routers, switches, hubs, and communication equipment shall be maintained in a secured location, such as a locked closet.
- b) All servers shall be maintained in a secured location, such as the data center or a locked closet within an ancillary department.

A. Information Asset Access Controls

Offices, computer rooms, and work areas containing *CONFIDENTIAL* information or information assets capable of accessing *CONFIDENTIAL* information shall be physically controlled. Management shall consult the site security group and the facilities engineering department to determine the appropriate access control method (receptionists, key-locks, magnetic card door locks, etc.). The following items shall be considered by site management when developing information asset access controls:


	Information Security Policies and Procedures	No. COMP-Sec 5.1.0
	Title: INFORMATION ASSET SECURED AREA PROTECTION STANDARD	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 11/03/00

- a) Electronic access control is the preferred method to secure areas;
- b) Manual access controls, such as key locks and cipher (push button) locks may also be used;
- c) Internal windows that could provide access to secure areas should be locked when unattended;
- d) Restricted areas shall be controlled 24 hours a day, with doors only left open/unlocked during working hours if the area is consistently occupied by members of the workforce; and
- e) Restricted area access points shall be electronically monitored during closed hours and alarmed to indicate if they are opened.

B. Data Center Protection

Data centers include any location within the hospital where one or more critical servers are maintained. Data centers shall apply appropriate physical security measures to protect the data center from common hazards such as intrusion, fire, flooding, etc. The minimum requirements established by the Federal Information System Controls Audit Manual (FISCAM) should be used as a guideline.

- a) Data centers should have automatic detection equipment installed to identify threats. The presence of these systems shall be complemented with monitoring. The following threats may be monitored:
 - (i) Fire (heat and smoke);
 - (ii) Water;
 - (iii) Humidity (high and low);
 - (iv) Temperature; and
 - (v) Power (spike and drop).
- b) Data centers should have a certified fire suppression system installed in accordance with local codes and ordinance.

	Information Security Policies and Procedures	No. COMP-Sec 5.1.0
	Title: INFORMATION ASSET SECURED AREA PROTECTION STANDARD	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 11/03/00

- c) Access to data centers shall be restricted to system administrators, system operators, and system support personnel.
- d) Data centers should have electronic access controls in place, and shall be alarmed. If possible, records shall be maintained of entries into the data center.

C. Data Center Structure


When addressing data center facility issues, it is recommended that:

- a) The data center be located above the first floor, away from windows, and not contiguous with kitchen or rest room facilities;
- b) There be no signs indicating the location of computer or communications centers;
- c) Walls be built to extend from existing base floor to the overhead deck;
- d) Walls surrounding computer facilities be non-combustible and resistant to fire;
- e) All openings to walls (doors, ventilation ducts, etc.) be self-closing; and
- f) Computer facility rooms be equipped with fire doors that:
 - (i) Close automatically;
 - (ii) Resist forcible entry;
 - (iii) Unlock automatically when a fire alarm is activated; and
 - (iv) Sound an alarm if opened for extended periods.

D. Intermediate Holding Area

A secured intermediate holding area shall be used for computer supplies, equipment, and other deliveries. Delivery personnel shall not be able to directly access rooms containing multi-user computer facilities.

E. Data Center Environmental Support Equipment

	Information Security Policies and Procedures	No. COMP-Sec 5.1.0
	Title: INFORMATION ASSET SECURED AREA PROTECTION STANDARD	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 11/03/00


Management shall provide and maintain power conditioning, air conditioning, and other computing environment protection systems necessary to assure continued service for critical computer systems, including:

- a) All servers within the data center(s) shall be connected to an uninterruptible power supply (UPS) system that shall:
 - (i) Allow administrator's time to do a soft shutdown of computing assets in case of a power outage;
 - (ii) Allow the backup generators or redundant commercial power source time to come on line without affecting the computing assets attached to the UPS (seamless power source transfer); and
 - (iii) Provide power conditioning such as spike protection and over/under voltage protection.
- b) Data centers shall have backup generator power sufficient to support the center for an extended period shall there be a catastrophic failure of power.
 - (i) Redundant generator capability is recommended to protect against equipment failure; and
 - (ii) Fuel reserves shall correspond to the danger of extended loss of power in each data center.
- c) Data centers shall have air conditioning with the ability to keep the computer room at the temperature and humidity standard set by the information asset manufacturers.
- d) The water supply for information assets or air conditioning systems shall have some form of redundancy.

F. Tape Library

Tape libraries should meet the same environmental requirements as those pertaining to the data center and shall not be contiguous to, or part of, the data center.

G. Smoking, Eating And Drinking

	Information Security Policies and Procedures	No. COMP-Sec 5.1.0
	Title: INFORMATION ASSET SECURED AREA PROTECTION STANDARD	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 11/03/00

Smoking, eating, and drinking in the data center or tape library shall be prohibited.

H. Infrastructure Facility Access

Access to infrastructure assets, including power generators, HVAC systems, and telephone/wiring closets should be restricted to authorized maintenance personnel only.

IV. RELATED DOCUMENTS AND REFERENCES

The following documents are directly related to this procedure, the Tenet:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0 and subordinate Standards and Procedures.
- Physical Safeguards for Information Assets Policy 5.0.0.
- Information Asset Open Area Protection Standard No. 5.2.0.
- Tenet Corporate Physical Security Policy.
- Site Specific Physical Security Policy.
- Tenet Human Resources Policies and Procedures No. 804 “Security Inspections”.