	Information Security Policies and Procedures	No. COMP-Sec 4.0.0
	Title: INCIDENT HANDLING POLICY	Page: 1 of 7
		Revised Date: 12/22/04
		Original Date: 09/29/00

Incident Handling Policy

I. SCOPE

This policy 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 policy applies to all Tenet information assets and information asset Users.

II. PURPOSE

Provide an organized approach for reporting and responding to information security incidents. The growing use of external data communications at Tenet has increased the likelihood of encountering threats to the security of systems and information. A structured approach is needed to respond to information security incidents and return systems to normal operation as quickly as possible.

III. POLICY

A. Security Incident Definition

An information security incident is an event or situation that poses a threat to the integrity, confidentiality, or availability of information or systems. These incidents violate corporate policies and may violate local, state and federal laws or regulations.


- a) The direct result of information security incidents may include information disclosure, modification, destruction or denial of system services.
- b) Indirect results of information security incidents may include loss of business, loss of computing capacity, violation of privacy, civil lawsuits, loss of public confidence, or adverse consequences to other computing assets.

Addendum A to this policy contains a list of Reportable Information Security Incidents that shall be used to report, track and evaluate the effectiveness of Tenet’s Information Security initiatives.

B. Security Incident Handling Priorities

Priorities for handling information security incidents are as follows:

- 1. Protection of human life and safety.
- 2. Protection of Tenet’s *CONFIDENTIAL* and *PROPRIETARY* information.

	Information Security Policies and Procedures	No. COMP-Sec 4.0.0
	Title: INCIDENT HANDLING POLICY	Page: 2 of 7
		Revised Date: 12/22/04
		Original Date: 09/29/00


3. Collection and analysis of information to determine if a violation of the Tenet Information Security Policies or the commission of a computer crime has occurred.
4. Prevention of damage to systems and restoration of systems to routine operation as quickly as possible.

Special procedures shall be followed in cases where Information Security incidents involve the disclosure of protected health information (PHI). For additional information on this topic, refer to Tenet's Privacy Policies and Procedures.

C. Information Security Incident Recognition

System Users may not readily recognize that a computer incident has occurred. These problems are frequently difficult to identify and require analysis to determine if there has been an incident and the impact of the incident. It is imperative for Users to report suspected incidents immediately. The following symptoms shall alert Users to the possibility of an information security incident:

- a) Unauthorized changes to file contents.
- b) Recorded use of a UserID when the authorized User was not accessing the system.
- c) Discrepancies in file sizes or dates.
- d) Computer virus infections.
- e) Changes in configurations and settings.
- f) Passwords that have changed or expired outside of the normal time periods.
- g) Observations of fellow employees making unauthorized copies (hard copy or electronic) of *CONFIDENTIAL* or *PROPRIETARY* information.
- h) Unknown individuals in an area or at a desk.
- i) Individuals without proper identification.

	Information Security Policies and Procedures	No. COMP-Sec 4.0.0
	Title: INCIDENT HANDLING POLICY	Page: 3 of 7
		Revised Date: 12/22/04
		Original Date: 09/29/00

- j) Inappropriate use of Tenet information assets, such as accessing non-business related Internet sites.

D. Reporting Information Security Incidents

All attempted or successful information security incidents, such as a break-in, intrusion, virus, or suspected illegal or unethical activity, shall be reported as quickly as possible.

When any individual observes or suspects the occurrence of an information security incident, they shall report the incident to the facility’s Security Officer, Privacy Officer and/or other Incident Response Team members (i.e. Facility Security). If an Incident Response Team member is made aware of a potential incident, he/she shall ensure that the appropriate actions are taken in response to the incident.

1. *INCIDENT RESPONSE TEAM*


The Incident Response Team is a team of managers, professionals and technicians with the authority and expertise to resolve a system incident. The members represented on the Incident Response Team may include:

Facility personnel:

- a) A member of the facility’s Administrative Management Team
- b) The facility’s Security Officer
- c) The facility’s Privacy Officer and/or Hospital Compliance Officer
- d) Information Systems Department, including Director Systems Administrator, Network Administrator, and/or Telecommunications Administrator
- e) Facility security
- f) Risk Management Department

Corporate departments:

- a) Privacy/Security Office
- b) Compliance Department

	Information Security Policies and Procedures	No. COMP-Sec 4.0.0
	Title: INCIDENT HANDLING POLICY	Page: 4 of 7
		Revised Date: 12/22/04
		Original Date: 09/29/00

- c) Law Department
- d) Information Systems Department
- e) Risk Management Department
- f) Public Relations Department

The Incident Response Team is responsible for verifying an incident, determining the impact and compiling the security incident reports. The Incident Response Team shall develop, modify, periodically update, and regularly test incident response procedures.

2. *INDIVIDUAL USER REPORTING RESPONSIBILITIES*


Interference With Reporting Of Security Problems - Any attempt to interfere with, prevent, obstruct, or dissuade an employee in their efforts to report a suspected information security problem or violation is strictly prohibited and cause for disciplinary action, up to and including dismissal and possible prosecution to the fullest extent of the law. Any form of retaliation against an individual reporting or investigating information security problems or violations is also prohibited.

Reporting Offensive Communications - Users shall NOT respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications.

- a) Tenet’s Corporate Privacy/Security Office shall be notified of all offensive communications.
- b) Users shall retain copies of messages, notes, or voice mail entries of this nature and turn them over to the Privacy/Security Department.

B. Responding to Information Security Incidents

When a possible information security incident is reported, the Incident Response Team shall investigate the incident, analyze available data, and resolve the incident. All data collected during the investigation shall be maintained to assess changes necessary to avoid future incidents, categorize the incident for reporting purposes, and identify responsible parties. When responsible parties are identified, the information shall be provided to the appropriate manager and/or Human Resources for follow-up as required.

	Information Security Policies and Procedures	No. COMP-Sec 4.0.0
	Title: INCIDENT HANDLING POLICY	Page: 5 of 7
		Revised Date: 12/22/04
		Original Date: 09/29/00

1. *INCIDENT RESPONSE PROCEDURES*

The Incident Response Team shall coordinate with systems administrative staff, facility management and other teams, as necessary, to ensure any loss of data or capability is minimized and the incident is satisfactorily resolved.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.
- Sanctions Standard No. 4.1.0.
- Incident Response Procedure No. 4.1.1.
- Tenet Administrative Policies and Procedure No. 2.25 “Security Incident Reporting”.
- Tenet Administrative Policies and Procedure No. 2.35 “Information Systems: Sensitivity, Confidentiality, and Appropriate Use”.
- Tenet Human Resources Policies and Procedures No. 108 “Confidentiality of Company Information”.
- Tenet Human Resources Policies and Procedures No. 408 “Performance Management”.
- Tenet Employee Handbook.
- Tenet Standards of Conduct.

ADDENDUM A
Reportable Information Security Incidents (not comprehensive)

1. Unauthorized Disclosure

- *CONFIDENTIAL* or *PROPRIETARY* information is disclosed without authorization.

2. System Incapacitation

- A system's ability to function is impaired by a high volume of activity from various sources.
- A resource such as power, network access, or routing tables is modified, degrading the system's ability to perform normal functions.
- A malicious code (virus, trojan horse, etc.) interferes with a system's operation.
- An asset is stolen, damaged, or destroyed.

3. System Tampering

- A UserID is employed to gain access to system administrative functions without prior authorization.
- A system weakness allows access to system administrative functions by unauthorized Users.
- A valid UserID is permitted to gain access to system administrative functions without authorization.
- Non-administrative personnel are allowed to perform administrative system functions.

4. Information Tampering

- A UserID is employed to gain access without authorization to password files, protected or restricted data, licensed applications, software, or restricted applications, software, and/or code.
- A system weakness allows unauthorized access to password files, protected or restricted data, licensed applications, software, or restricted applications, software, and/or code.
- A theft of information assets provides access to password files, protected or restricted data, licensed applications, software, or restricted applications, software, or code.

5. Misuse of Information Technology

- A User installs unlicensed software.
- A User's account is employed in violation of legal statutes, regulations, or organization policies.

6. Unauthorized Access

- A valid UserID is employed without authorization.
- A system weakness is exploited, but no access is gained outside the account's authorizations.
- A User's privilege to access information is higher than that which was authorized.
- Access to facilities (buildings, rooms, secure areas) is gained without authorization.
- A User's laptop or desktop computer is stolen.

7. Unauthorized Use

- Any use of *CONFIDENTIAL* or *PROPRIETARY* information for a purpose not specifically permitted based on the User's need to know.

8. Attempted Exploration of Information Assets

- Illegal data gathering is directed against a system (port scanning, sniffing, net scanning, etc.).
- Actions are attempted that could impair a system's ability to function.
- Actions are attempted that could result in a system or information compromise.

9. Non-System Incidents

- Physical Facility Access Incidents – Unauthorized access to facilities results in information asset exposure or compromise.
- Physical Access to Information – Unauthorized parties gain access to *CONFIDENTIAL* or *PROPRIETARY* information.
- Equipment Control Incidents – Tenet information assets are exposed or compromised due to a lack of control over computing equipment.
- Media Control Incidents – Tenet information assets are exposed or compromised due to a lack of control over computing media.
- Physical Safeguards/Environmental Hazards – Tenet information assets are exposed or compromised due to an environmental hazard such as a tornado or thunderstorm.