	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 1 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

Incident Response 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 Users.

II. PURPOSE

To provide an organized approach for responding to information security incidents. A structured approach is necessary to adequately respond to information security incidents, quickly return operations and systems to a normal state, and prevent recurrences.

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


Information security incidents include a wide variety of illicit or careless actions such as:

A. Information Security Incidents

1. System Incidents.

Those incidents that involve an attack or an occurrence on an actively operating computer system. For example:

- a) An unauthorized person accessing Tenet’s Information Assets.
- b) A malicious code (e.g., virus, trojan horse, etc.) interferes with a system’s operation.
- c) A system weakness allows access to system administrative functions by unauthorized Users.
- d) 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 application code.

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 2 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- e) A User's laptop or desktop computer is stolen.
- f) Misuse of information assets.


2. Non-system Incidents.

Information security incidents that do not involve actively operating computer systems, but expose Tenet CONFIDENTIAL and PROPRIETARY information assets, are characterized as non-system incidents. Examples of these incidents include:

- a) **Physical Facility Access Incidents:** Information assets are compromised by persons obtaining unauthorized access to physical facilities such as computer rooms, medical records storage areas, or nursing units.
- b) **Physical Access to Information:** Information assets are compromised by persons obtaining unauthorized access to documents or information assets that contain Tenet CONFIDENTIAL or PROPRIETARY information.
- c) **Equipment Control Incidents:** Information is compromised due to failure of equipment control procedures; for example, a hard disk is taken out of service and given to an outside agency without the content being properly removed.
- d) **Media Control Incidents:** Information asset media is stolen, destroyed, accessed or otherwise exposed to unauthorized actions.
- e) **Physical Safeguards:** Occurrences involving natural disasters or environmental hazards that expose Tenet information assets to unauthorized persons.

3. Remediation methods depend on the scope, seriousness, priority and remediation options. Minimum steps required for remediation of any reportable information security incident shall include:

- a) Notifying Corporate Information Privacy/Security Office.
- b) Collecting data.
- c) Analyzing the data and situation.
- d) Establishing priorities.

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 3 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- e) Containing/resolving the incident.
- f) Returning to normal operation (whether a system or operating process).
- g) Performing post-incident activities (reporting and prevention of future incidents).

B. Incident Response

Upon receiving notification of an information security incident or suspected incident (system or non-system) the Incident Response Team shall begin the process of investigating the incident in a timely manner. The team or the investigator assigned to the incident may request any or all of the following:

- a) A system snapshot that provides a baseline comparison allowing identification of continuing changes.
- b) Backups of the online storage media relevant to the system.
- c) Collection and protection of applicable audit trails or system logs.
- d) Exception reports generated from detailed system logs.
- e) System monitoring reports.
- f) Documentation of the affected system and its connectivity.


C. System Incident – Procedure

The following steps shall be taken when responding to a system information security incident.

1. Notify Appropriate Parties

Multiple parties should be notified of a system security incident and should be frequently updated as to the progress of the response process. The Incident Response Team handling an incident should:

- a) Notify facility management and Corporate Information Privacy/Security Office of the incident. This initial notification will allow these parties to track and

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 4 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

report incidents appropriately, and will promote discussion of corrective action recommendations.

- b) Frequently update the facility's Incident Response Team and Corporate Information Privacy/Security Office on the progress of the incident response process. These updates should include a description of any corrective actions taken to resolve the incident and to prevent future recurrences.
- c) Submit any additional documentation or reports to other individuals within the facility as required by the facility's internal procedures for incident reporting. Coordinate with the Corporate Information Privacy/Security Office to communicate to Tenet's Clinical Quality, Risk Management and Law Department teams as necessary and follow-up to assure appropriate corrective actions are completed.

2. Start a Log

Record all information related to the incident on an Incident Event Chronology Form (Addendum A) or in similar documentation, including:


- a) Dates, times, people, locations, phone calls, meetings, discussions, research, and other investigative actions; and
- b) All response, recovery, and follow-up activity.

3. Analyze Preliminary Information

Determine the type, severity, scope and impact of the incident, including:

- a) The number of sites and systems involved;
- b) The classification (*CONFIDENTIAL, PROPRIETARY, PUBLIC*) of the data involved;
- c) The method used by the intruder to gain access;
- d) Whether the intrusion continues; and
- e) An estimation of the time and resources needed to resolve the incident.

4. Capture and Record Data

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 5 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

Based on the analysis, capture any additional required data not gathered at the beginning of the incident investigation.

5. Establish Priorities

Prioritize actions necessary to resolve the incident according to the guidelines as described in the Information Security Incident Handling Policy 4.0.0.


6. Contain the Incident

To prevent further damage, destruction of evidence, exposure of information, or the use of Tenet systems to attack other systems, contain the incident. This may take many forms, including:

- a) Forcefully end a User's session;
- b) Change a User password;
- c) Change all passwords;
- d) Stop a particular service, or stop all services (not a complete system shutdown);
- e) Disconnect a system from the network;
- f) Shutdown a system and apply patches to remedy the problem; and
- g) Shutdown a system and reload all programs and data from a known, good backup.

Some of these decisions can lead to a loss of data and/or production time and shall require facility management approval.

- a) Other steps that may be necessary to contain the attack include:
 - (i) Informing Users of an unexpected shutdown and time to return to service. This allows Users to begin using contingency planning procedures if necessary;

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 6 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- (ii) Performing a complete backup. Produce two (2) backups if evidence is needed for legal authorities (write-protect or write-once media shall be used) and for selective restoration of files;
- (iii) Eradicating the problem or damaged files. If available, use a file comparison utility to compare the compromised system with the previous status and delete and restore selected files. If no comparison can be performed, a complete restoration of the system from a trusted source may be required;
- (iv) Checking pre-existing backups to ensure they do not contain damaged files, viruses, malicious software etc;
- (v) Ensuring any redundant systems and/or data have not been compromised;
and
- (vi) Ensuring other (networked) systems have not been compromised.

7. Disaster Recovery

During the course of an incident, it may become necessary to turn the incident over to the disaster recovery team. Thereafter, all Information Security Incident Response Procedures shall become subordinate to the Disaster Recovery Team efforts.


8. Gather Evidence

If a crime has occurred:

- a) Secure all evidence to ensure a chain of custody.
- b) Facility management shall work with legal counsel to determine whether to refer the incident to legal authorities.

9. Notify Third Parties

Only management, such as the facility CEO, CIO, CFO, or a Corporate Officer may authorize the release of information related to an information security incident to a third party. Entities that may be contacted with this authorization include:

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 7 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- a) Federal, State or local law enforcement or other agencies per laws and regulations.
- b) A third party directly affected by the incident to enable them to perform remedial action on their systems.
- c) No statements to the press shall be made. All inquiries shall be directed to the Public Relations Department.

10. Restore the System


If this step is performed before intrusion analysis and corrections to system security have been completed, those actions shall be completed as soon as possible. Steps to return to normal operation shall vary between systems, but may include:

- a) Restoring the operating system; reconfigure to fix the security problems (change management procedures);
- b) Correcting or restricting the methods used to create the incident;
- c) Restoring programs;
- d) Restoring User data from trusted backup media; and
- e) Reviewing system configurations including User accounts, system services, audit and monitoring facilities, and access control lists. Comparing all system configuration files to authoritative copies of these files or compare cryptographic checksums with trusted checksums collected before an intrusion.

11. Return to Normal Operations

Reconnect the restored system to the network. This may include multiple steps, including:

- a) Validating the restored system;
- b) Reviewing all restored data files that resided on the compromised system to ensure they were not affected by an intruder's activities; and

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 8 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- c) Monitoring the restored system for failed login attempts, attempts to access back doors, attempts to re-exploit the original vulnerability, and attempts to exploit new vulnerabilities.

12. Update Network Protection


All protection mechanisms (such as firewalls, intrusion detection systems, etc.) shall be reviewed and their configurations adjusted based on incident analysis, including:

- a) Determining if protection mechanisms need to be configured differently;
- b) Determining if protection mechanisms need to be placed in a new or additional location on the network;
- c) Reviewing recent information on vulnerabilities, patches and new versions of protection mechanism software, to ensure the system has adequate protection;
- d) Updating the mechanisms to ensure that similar attacks are detected or dealt with in the future; and
- e) Reviewing and updating the conditions under which detection mechanisms generate alerts to system and network administrators and forms in which the alert is made (e-mail, phone, page, etc.).

13. Improve Processes

The actions taken after an incident allow Tenet to take steps to counter the behaviors that caused the incident, including:

- a) Monitoring the system to ensure the system is restored to normal and no back doors or “traps” exist;
- b) Performing an inventory of the system and network assets;
- c) Determining if there are vulnerable systems or network vulnerabilities, and taking action to correct them;
- d) Conducting a security audit or evaluation of the system;
- e) Resolving improper access to systems and resources;

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 9 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

- f) Performing a complete backup of the system to ensure changes can be quickly reapplied;
- g) Developing a set of “lessons learned” for future security efforts and performance in handling incidents;
- h) Documenting actions taken to resolve the incident/attack for use in response to possible future incidents/attacks; and
- i) Performing a risk analysis based on the severity and impact of the incident, answering the following:
 - (i) Were the policies and procedures adequate?
 - (ii) What methods of discovery and monitoring procedures would have improved Tenet’s ability to detect this incident?
 - (iii) What tools or procedures would have made responding to this incident easier or quicker?
 - (iv) What tools or procedures would have enhanced Tenet’s ability to contain this incident?
 - (v) What was the loss in monetary damages and downtime?


14. Document

Document the events surrounding an incident and the actions taken in response to an incident on an Incident Event Chronology Log Form (Addendum A) or in similar documentation. Document corrective actions taken on a Corrective Action Plan (Addendum B).

D. Non-System Incident – Procedure

The following steps shall be taken when responding to a system information security incident.

1. Notify Appropriate Parties

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 10 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

Multiple parties should be notified of a system security incident and should be frequently updated as to the progress of the response process. The Incident Response Team handling an incident should:

- a) Notify facility management and Corporate Information Privacy/Security Office of the incident. This initial notification will allow these parties to track and report incidents appropriately, and will promote discussion of corrective action recommendations.
- b) Frequently update the facility's Incident Response Team and Corporate Information Privacy/Security Office on the progress of the incident response process. These updates should include a description of any corrective actions taken to resolve the incident and to prevent future recurrences.
- c) Submit any additional documentation or reports to other individuals within the facility as required by the facility's internal procedures for incident reporting. Coordinate with the Corporate Information Privacy/Security Office to communicate to Tenet's Clinical Quality, Risk Management and Law Department teams as necessary and follow-up to assure appropriate corrective actions are completed.

2. Start a Log


Record all information related to the incident on an Incident Event Chronology Form (Addendum A) or in similar documentation, including:

- a) Dates, times, people, locations, phone calls, meetings, discussions, research, and other investigative actions; and
- b) All recovery, follow-up and response activity.

3. Collect and Analyze Data

Gather data necessary to evaluate the incident and determine the best course of action to meet Tenet's incident handling priorities. Use the preliminary information to determine the type, scope and impact of the incident.

4. Establish Priorities

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 11 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

Using the organization's overall guidelines for incident handling priorities described in the Information Security Incident Handling Policy, the Incident Response Team shall prioritize actions to resolve the incident.

5. Contain the Incident

Ensure the necessary steps are taken to conclude the incident. Including:


- a) Locking doors;
- b) Securing information assets;
- c) Locating missing equipment or media;
- d) Initiating an internal investigation;
- e) Initiating disciplinary action;
- f) Arranging for Information Security Awareness training;
- g) Communicating with the facility disaster recovery team in the case where an environmental hazard has led to a disaster situation;
- h) Halting work processes that expose the facility to undue risk of information exposure; and
- i) Escorting unauthorized visitors from the building or area.

6. Gather Evidence

If the incident involves the commission of a crime or suspected crime, the appropriate facility management shall be notified. Referrals to legal authorities shall be performed by the appropriate Facility or Corporate officers in conjunction with the Law Department.

7. Document

Document the events surrounding an incident and the actions taken in response to an incident on an Incident Event Chronology Log Form (Addendum A) or in similar documentation. Document corrective actions taken on a Corrective Action Plan (Addendum B).

	Information Security Policies and Procedures	No. COMP-Sec 4.1.1
	Title: INCIDENT RESPONSE PROCEDURE	Page: 12 of 14
		Revised Date: 01/11/06
		Original Date: 10/02/00

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Sanctions Standard No. 4.1.0.
- Incident Handling Procedure No. 4.1.1.
- Tenet Administrative Policies and Procedures No. 2.25 “Security Incident Reporting”.
- Tenet Administrative Policies and Procedures 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.

