	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 1 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

Logging and Auditing 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 logging and auditing requirements. Logging and auditing of actions within networks, systems, and applications supports the security initiatives for information assets owned by Tenet.

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

Administrators of Tenet information assets shall log certain activities that occur on networks, systems, and applications. These logs shall provide sufficient data to support incident investigation and comprehensive audits of compliance with the Information Security Policies and Procedures. Logging and auditing shall be implemented using the following guidelines:


A. Activity Logs and Audit Trails

There are certain activities that occur on networks, systems and applications that shall be logged. These include, but are not limited to, activities such as data requests, data transfers, changes to configuration files, and the addition, deletion or modification of a UserID.


Logs of computer security events shall provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with, the Information Security Policies and Procedures.

1. Security Event Logging Detail

Logs shall be created that can be used to monitor activities that can affect network, system or application security. These logs shall record the following:

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 2 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

- a) Intrusion activity
 - (i) Failed login attempts with an invalid UserID
 - (ii) Failed login attempts with a valid UserID (password guessing attempts)
 - (iii) Failed password change attempts
 - (iv) Attempts to use privileges that have not been authorized
- b) UserID administration activity
 - (i) Modifications
 - (ii) Additions
 - (iii) Deletions
 - (iv) Disabling
 - (v) Re-enabling
 - (vi) Changes to the privileges of users
- c) System activity
 - (i) Start-up
 - (ii) Shut-down
- d) Hardware
 - (i) Hardware and disk media errors
 - (ii) Maintenance activity
- e) System anomalies
 - (i) Initialization sequences

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 3 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

- (ii) Logons and errors
- (iii) System processes and performance
- (iv) System resources utilization

2. Perimeter Protection Logging Detail


Logs shall be created that can be used to monitor activities on perimeter devices, including firewalls and routers. These logs shall record the following:

- a) Device activity
 - (i) Packet screening denials originating from trusted and un-trusted networks
 - (ii) User account management
 - (iii) Modification of packet filters
 - (iv) Application errors
 - (v) System errors
 - (vi) System shutdown and reboot


3. User Activity Logging Detail

Logs shall be created in such a manner that individual events are attributed to individual UserIDs. Networks and applications shall log activity using the following guidelines:

- a) User activity should be logged at the field level, and shall record the following:
 - (i) UserIDs
 - (ii) Access date/time
 - (iii) User Access
 - (1) Record access

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 4 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

- (2) Field access
- (iv) User Actions
 - (1) Additions at the record and field level
 - (2) Modifications at the record and field level
 - (3) Deletions at the record and field level
- b) If user activity cannot be logged at the field level, activity logging should be maintained at the record level, and shall record the following:
 - (i) UserIDs
 - (ii) Action date/time
 - (iii) User Access
 - (1) Record access
 - (iv) User Actions
 - (1) Additions at the record level
 - (2) Modifications at the record level
 - (3) Deletions at the record level
- c) If user activity cannot be logged at the record level, activity logging should be maintained at the system access level and this decision should be documented in the facility's Information Security Control Exceptions Book. User activity at the system access level shall be recorded, including:
 - (i) UserIDs
 - (ii) Logon date/time
 - (iii) Logoff date/time

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 5 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

- (iv) Password change date/time
- (v) Applications invoked
- (vi) Attempted access to unauthorized data
- (vii) Use of authorized advanced privileges (security bypass, etc)
- (viii) Changes to critical application system files
- (ix) Modifications

4. Backup, Archive, And Protection


Log files shall be saved to tape or other media and secured in off-site or other appropriate storage. Log files shall be backed up according to this procedure and the Backup Procedure No. 8.2.3.

- a) Logs shall be rolled (a new log activated, the old log saved) rather than being overwritten (the same log is used again, losing data).
- b) Log files are CONFIDENTIAL and shall be protected such that no individual can modify or delete the logs.
- c) Individuals authorized to view logs include members of the internal audit staff, systems security staff, or systems management staff.
- d) If an unauthorized individual needs access to these logs, they shall request access in writing and obtain written permission from facility management.

5. Backup Retention

Log files shall be retained for a period of time so as to accomplish their purpose, and according to the following guidelines:

- a) Activity logs shall be retained as specified by Tenet's Records Management Policy or contractual, regulatory, or statutory mandates.
- b) It is recommended that security event and user activity logs be retained for a period of one (1) year. If log files cannot be retained for one (1) year, log files

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 6 of 7
		Revised Date: 12/22/04
		Original Date: 01/17/01

shall be maintained for no less than ninety (90) days, and this decision should be maintained in the facility's Information Security Control Exceptions Book.

6. Clock Synchronization

The internal clocks of systems that generate activity on Tenet networks and applications shall reflect the current time accurately.

The Corporate Information Systems Department shall provide the functionality for clock synchronization.

7. Deactivation, Modification, or Deletion

Mechanisms to detect and record significant computer security events shall be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.


B. Audit Log Reviews

System Administrators and/or security Administrators shall monitor the security event logs created by the facility information assets to ensure that inappropriate behavior or potential intrusions are recognized and addressed.

- a) Audit logs shall be examined for failed logon attempts and other security events on a routine basis. It is recommended that this be conducted daily, or at a minimum every fourteen (14) days.
- b) Automated utilities may be used to assist in audit log reviews. However, manual reviews should be conducted periodically to identify unusual, unexpected or suspicious behavior not identified through automated reviews.
- c) It is recommended that reviews of user activity also be conducted if such reviews could assist in identifying unusual, unexpected, or suspicious behavior.
- d) Centralized monitoring is preferred over individual system monitoring.

2. Incident Reporting and Notification

Any incidents found in the log auditing procedure shall be handled according to the Incident Handling Policy 4.0.0 and its subordinate Standard and Procedures.

	Information Security Policies and Procedures	No. COMP-Sec 8.2.2
	Title: LOGGING AND AUDITING PROCEDURE	Page: 7 of 7
		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.
- Incident Handling Policy No. 4.0.0 and its subordinate Standard and Procedures.
- Contingency Planning Policy No. 6.0.0 and its subordinate Standard and Procedures.
- Security Risk Management Standard No. 7.1.0.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0.
- Change Control Procedure No. 8.2.1.
- Backup Procedure No. 8.2.3.
- 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 Administrative Policies and Procedures No. 1.11 “Records Management”.
- Tenet Human Resources Policies and Procedures No. 306 “Records Retention”.