	Information Security Policies and Procedures	No. COMP-Sec 8.3.5
	Title: PRIVATE BRANCH EXCHANGE (PBX) AND VOICE MAIL PROCEDURE	Page: 1 of 5
		Revised Date: 12/22/04
		Original Date: 01/15/00

Private Branch Exchange and Voice Mail 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 guidelines for the use of system Administrators to secure Tenet’s PBX and voice mail systems. Telephone and voice mail systems can lead to inadvertent exposure of information assets, fraud and financial losses for Tenet. Proper configuration and management of these assets shall reduce this risk.


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

The first step in improving PBX security is to assess the facility’s current telephony applications. Once the applications are assessed, Administrators shall ensure that the systems are configured to enhance information security. PBX and voice mail systems are subject to the following threats:

- a) Theft-of-service (toll fraud).
- b) Disclosure of information (eavesdropping and unauthorized access).
- c) Data modification (modification of system tables to gain additional services)
- d) Unauthorized access (actions that permit unauthorized Users to gain access to system resources or privileges).
- e) Denial of service (actions that prevent the system from functioning in accordance with its intended purpose).

A. PBX Maintenance

	Information Security Policies and Procedures	No. COMP-Sec 8.3.5
	Title: PRIVATE BRANCH EXCHANGE (PBX) AND VOICE MAIL PROCEDURE	Page: 2 of 5
		Revised Date: 12/22/04
		Original Date: 01/15/00

PBXs typically require remote maintenance by the vendor. This requires access to the switch by a potentially large pool of outside parties. Access to these switches shall be tightly controlled. Maintenance features may include the following:

- a) Database upload/download utility.
- b) Database examine/modify utility.
- c) Software debugger/update utility.

To control access to remote maintenance, dial-back modems along with these additional countermeasures shall be employed:

- a) Ensure remote maintenance access is normally blocked unless unattended access is required.
- b) If possible, install two-factor, strong authentication on remote maintenance ports.
- c) Keep maintenance terminals in a locked, restricted area.
- d) If possible, turn off maintenance features when not needed.


B. PBX Administrative Databases

Administrative databases represent “the key to the kingdom” for a PBX. Creation and modification of user databases and the operating software controlling the switch are the most critical functions of the PBX Administrator.

- a) Passwords: Access to system maintenance and administrative functions shall be allowed only with a UserID and password. Factory default values shall be changed.
- b) Physical Security: All components of the PBX system (switches, terminals, software, other peripheral units) shall be contained in a secure location.

C. Automatic Call Distribution (ACD)

ACD allows a PBX to be configured so that incoming calls are distributed to the next available operator or placed on hold until an operator becomes available. Vulnerabilities

	Information Security Policies and Procedures	No. COMP-Sec 8.3.5
	Title: PRIVATE BRANCH EXCHANGE (PBX) AND VOICE MAIL PROCEDURE	Page: 3 of 5
		Revised Date: 12/22/04
		Original Date: 01/15/00

exist if an adversary gains access to the configuration tools or the system database. Access to these tools shall be tightly controlled.

D. Account Codes/Authorization Codes

Account Codes are normally used for tracking calls made by certain people or projects so that bills can be charged appropriately.

- a) Account codes should be required for making long-distance calls from facility phones.
- b) Account codes should be protected in the same manner as UserIDs and passwords.
- c) Reports used to review call records for billing purposes should be stored in a secure location and disposed of in a secure manner.

Dial In System Access (DISA) allows Users to dial in to the PBX system from an outside line and gain access to the normal features of the PBX. This feature shall be inactivated, if possible.

E. Override (Intrude) Features


Override is intended to allow one user (perhaps a supervisor) to break into a busy line to inform another user of an important message. The PBX shall provide for some protection against uses of Override by providing visual and/or audible warnings that an Override is in progress.

F. Diagnostic Features

The interaction between features presents a significant possibility for vulnerabilities. Vulnerabilities may exist that were undetected by the manufacturer that allow unwanted access to the PBX and its instruments. The most effective strategy to defend against unwanted access is to ensure that only essential PBX features are activated.

G. Computer Telephony (CT)

A CT system typically requires only the addition of specialized voice processing boards to an ordinary office PC. Use of CT systems increase integration of telephony with the computer network and vulnerabilities are greatly expanded. CT features that may be at risk include:

	Information Security Policies and Procedures	No. COMP-Sec 8.3.5
	Title: PRIVATE BRANCH EXCHANGE (PBX) AND VOICE MAIL PROCEDURE	Page: 4 of 5
		Revised Date: 12/22/04
		Original Date: 01/15/00

- a) Voice over IP.
- b) Browser-based call handling and administration.
- c) Integration of IP PBX with legacy PBXs and voice mail systems.
- d) Integration of wireless networks with office network systems.
- e) Virtual private networks.


The safest course of action is to assume that most or all of the vulnerabilities inherent to a PBX system apply to a CT system as well. CT systems also have added vulnerabilities resulting from well-known weaknesses of PC operating systems.

As with PBX systems, the first step in securing a CT system is to assess system configuration against risks to determine corrective measures.

H. Voice Mail

Voice mail systems are to be secured with a confidential password known only to the mailbox owner.

- a) Remote access to the Voice Mail configuration for system administration purposes shall not be allowed.
- b) Security awareness initiatives shall be implemented to reduce fraudulent activity through “social engineering” tactics.
- c) Administrators in charge of Tenet voice mail systems shall ensure that collect and third party bill-to calls are prohibited on voice mail telephone lines.
- d) The ability to transfer to an “extension” and create an outside call from a voice mailbox shall be blocked.
- e) Authorized voice mailboxes shall not be allowed to remain dormant for an extended time.
- f) Voice mail configuration shall require system-enforced password change to retrieve voice mail or modify features of the mailbox.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.5
	Title: PRIVATE BRANCH EXCHANGE (PBX) AND VOICE MAIL PROCEDURE	Page: 5 of 5
		Revised Date: 12/22/04
		Original Date: 01/15/00

- g) Care shall be taken when allowing the voice mail system to allow callers from transferring to another extension or the operator.
- h) Passing through the voice mail system to phone numbers or extensions that start with 7, 8, or 9 that are normally used to make outside calls shall be restricted.
- i) A recovery plan shall be in place in case the voice mail system is not available due to an accident or malicious intent.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- User Security Policy No. 3.0.0.
- User Conduct Standard No. 3.3.0.
- Security Risk Management Standard No. 7.1.0.
- Tenet Administrative Policies and Procedures No. 2.18 “Coordination of Information Processing Systems”.
- Tenet Administrative Policies and Procedures No. 2.1 “Capital Expenditure Review Process”.