	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.4.0</b>
	<b>Title: OPERATING SYSTEM SECURITY STANDARD</b>	<b>Page: 1 of 14</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/24/01</b>

**Operating System Security 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 Tenet information assets and information asset Administrators.

**II. PURPOSE**

Provide direction for administration and maintenance of operating system security for Tenet information assets. Information Systems Administrators and other individuals shall apply these standards to ensure a consistent level of information security across Tenet information assets.

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. STANDARD**


A. Naming Standards

The following naming standard shall be used for servers.

- a) AAA=COMPANY (TEN=TENET)
- b) BBB=FACILITY (TSC=TENET SERVICE CENTER)
- c) CCC=OPERATING SYSTEM OR PRIMARY APPLICATION (WNT=WINDOWS NT)
- d) ##=SERVER NUMBER (01=SERVER 01)
- e) Separate each with an underscore (\_)
- f) Example = TEN\_TSC\_WNT\_01

B. Administration

Administrators shall:


	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.4.0</b>
	<b>Title: OPERATING SYSTEM SECURITY STANDARD</b>	<b>Page: 2 of 14</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/24/01</b>

- a) Consider security impacts and configurations in the beginning of the system design process.
- b) Follow the Change Control Procedure No. 8.2.1 to obtain approval from facility management and the Corporate Information Systems Department before establishing servers.
- c) Configure assets so that no single person can make an error or manipulate the records without such events being detected.
- d) Use and support standard naming conventions for UserID (See UserID Control Procedure No. 8.1.1) codes, production program names, production file names, and system names.
- e) Maintain the operating system configuration.
  - (i) Apply security patches provided by operating system vendors.
  - (ii) Monitor resources to identify newly released information about threats and vulnerabilities.
  - (iii) Upgrade the version of the operating system when appropriate.
- f) Users shall be configured to perform their work through a series of menus or icons to restrict access to the operating system commands.
- g) Perform regular preventive maintenance on all information assets.
  - (i) Repairs and servicing of equipment shall be performed only by authorized maintenance personnel.
  - (ii) Preventive maintenance shall be performed at the vendor's recommended service intervals and maintenance specifications.

C. Access to Utilities

Access to systems software utilities shall be restricted to a limited number of technical personnel. Whenever these utilities are executed, the resulting activity shall be securely logged.

D. Access to Broadcast Tools

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.4.0</b>
	<b>Title: OPERATING SYSTEM SECURITY STANDARD</b>	<b>Page: 3 of 14</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/24/01</b>

Broadcast tools found in computer asset operating systems, e-mail systems, voice mail systems, and others, shall only be used by system Administrators or with facility management approval.

E. Last Logon Time and Date

Subject to system limitations, Users shall be provided information reflecting the last logon time and date when they logon to a system. This information shall be presented at the time of a successful User logon allowing unauthorized system usage to be detected.

F. System Logoff

All logoff procedures shall be configured so that the display screen at the User's terminal or workstation is cleared (blanked) after logoff procedures are completed.

G. Operating System Procedures


The following addendums provide guidelines for the configuration and maintenance of operating systems. Administrators shall use these guidelines with caution and in conjunction with system specific resources to develop site and system specific procedures and checklists for the secure configuration and operation of information assets.

- a) Addendum A: NT Administrative Procedure
- b) Addendum B: AS/400 Administrative Procedure
- c) Addendum C: Unix Administrative Procedure

**IV. RELATED DOCUMENTS AND REFERENCES**

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Record Processing Policy No. 2.0.0 and its subordinate Standard and Procedure.
- Information Access Control Standard No. 3.1.0 and its subordinate Procedures.
- Physical Safeguards for Information Assets Policy No. 5.0.0 and its subordinate Standards.
- Contingency Planning Policy No. 6.0.0 and its subordinate Standard and Procedure.

	<b>Information Security Policies and Procedures</b>	<b>No. COMP-Sec 8.4.0</b>
	<b>Title: OPERATING SYSTEM SECURITY STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Revised Date: 12/22/04</b>
		<b>Original Date: 01/24/01</b>

- Security Risk Management Standard No. 7.1.0.
- Technical Security Management Policy No. 8.0.0.
- Asset Access Controls Standard No. 8.1.0 and its subordinate Procedures.
- Information Asset Administration Standard No. 8.2.0 and its subordinate Procedures.
- 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”

## ADDENDUM A

### WINDOWS OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

#### WINDOWS (NT-BASED) SECURITY

The following information provides an overview of current known risks and vulnerabilities that need to be addressed to provide a standard level of information security controls for Tenet information assets. Individual Administrators shall use system specific resources to obtain and customize information security checklists to accomplish this goal.

##### A.1 Protect the System from Undesirable Booting

When appropriate:

- Set the “boot sequence” to start with the hard drive “C”.
- Disable the floppy drive and CD ROM.
- Set a BIOS password.
- On servers that allow it (IBM servers are one example), set “network node” in the BIOS so that the computer can restart but the keyboard is locked until the BIOS password is entered.

##### A.2 File System

FAT partitions shall be used for key boot files boot.ini, ntldr, nt detect.com, bootsect.dos (if you are using FAT partitions) and ntbootdd.sys (required only if you use SCSI disks) and the %systemroot% directory.

- All other files shall be under NTFS.
- Consider separate partitions for operating systems/applications and Users files.
- Change permissions that the Everyone group has to directories throughout the file system to “Read”.
- Review and tighten security on the profiles directory, temporary directories, audit logs, system root\repair directory, boot.ini, ntldr, all executable files, and all shared directories.

##### A.3 Emergency Repair Disks

Create Emergency Repair Disks (ERD) after the system is up and operating, just before being placed into production.

- These disks can be used to violate the system (they contain a copy of the SAM database). Set up a locked storage area for the emergency disks.

- The command shall include the /s switch to capture the current SAM.
- After new emergency repair disks are made, delete out of date information in the \winnt\repair directory.
- The ERDs shall be updated any time a system or application change takes place.

#### A.4

#### Registry

Inappropriate access to the registry may cause the loss of the entire Windows asset.

- Set the ACLs to protect sensitive parts of the Registry.
- Set the “Everyone” (or Authenticated Users) group to Read for the Registry keys that are being changed in this process.
- When possible, use the System Policy Editor rather than editing the registry.
- When adding a new entry, use the function “Add Value” rather than the more intuitive “Add Key” function. “Add Key” can cause unexpected events.
- Delete the entry DefaultPassword if it is present.
- Turn on the Legal Notice Caption; see the Asset Access Controls Standard No. 8.1.0 for the text. Telnet and FTP need to show similar notices.
- Enforce strong passwords (registry portion), use the password filter DLL provided with Service Pack 3. See the Password Control Procedure No. 8.1.2 for further information.
- Consider disabling automatic restart after outage, the business impact shall be considered.
- Control remote access to the registry.
- Allow scheduling commands to be submitted by system operators.
- Restrict anonymous network access to the registry and to lookup account names, groups, and shares.
- Encrypt Sam’s Password Database With 128 Bit Encryption.
- Secure the event log.
- Enable audits of backups and restores.

- Manage log files, see Logging And Auditing Procedure No. 8.2.2 for further details on this subject.

#### A.5 User Accounts and Password Restrictions

Set up User accounts, and set the Account Policy password restrictions dialog box to support the:

- Asset Access Controls Standard No. 8.1.0
- Information Access Control Standard No. 3.1.0
- Access Request And Modification Procedure No. 3.1.1
- Administrator Account, consider:
  - o Renaming the account.
  - o A complex password.
  - o Restrict distribution.
  - o Administrators shall review and consider using the Passprop.exe utility.
  - o Administrators shall get individual accounts with essentially the same permissions but without the no-lockout feature built into the Administrator account.
- System Account: The System account is an internal account that does not show up in the User Manager, cannot be added to any groups, and cannot have its rights changed. Some services will only run under the System account, such as Server and Workstation.
  - o When installing a new service, run that service under a special account that has the lowest level of access rights and permissions that the service requires AND under a local account rather than a domain account.
- Same Name Local Accounts: Local accounts with the same name on different machines shall use different passwords.
- Guest Account: TENET requires that all NT machines have their guest account disabled, regardless of the machine's function.

#### A.6 Groups

Groups shall be used to manage the rights and permissions of Users rather than the individual User account.

- Global groups shall be reviewed on a regular basis.
- The guest group in any master domain shall be disabled.
- Replace the User “Everyone” with “Authenticated Users” in all shares and directories that require common access. Set the RestrictAnonymous key before completing this action.

#### A.7 Internet Security Settings

Extreme care shall be taken with IIS both in configuration and in monitoring and installing patches.

- Disable use of clear text passwords and directory browsing.
- Install IIS on its own server when possible, separated from other enterprise information. Alternatively, some sites set up separate partitions for their NT system files, their web scripts, and their HTML documents. In the least, use read-only directories for HTML and Execute only for server side executables.

#### A.8 Rollback

Microsoft inadvertently distributed ROLLBACK.EXE on some Windows NT version 4.0 servers and workstation CDs. When executed, ROLLBACK destroys critical system information including the Registry, User account information, and more. The only fix to this problem is to restore the entire system from a current tape back up, providing one is available. The Emergency Repair Disk can't restore the system since it requires the SETUP.LOG and Registry components that ROLL BACK.EXE deletes.

- Check for ROLLBACK.EXE on the hard disk and if it is present, remove it.

## ADDENDUM B

### A/S 400 OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

#### AS/400 SECURITY

The following information provides an overview of current known risks and vulnerabilities that need to be addressed to provide a standard level of information security controls for Tenet information assets. Individual Administrators shall use system specific resources to obtain and customize information security checklists to accomplish this goal.

##### B.1 Protect the System from Undesirable Booting

Every system unit has a control panel that can be used to service the machine and to perform special operations, such as powering the system on and off.

- Every system unit also has a key lock switch that can prevent unauthorized use of these system functions.
- The recommended setting is **NORMAL**.

##### B.2 System Values

The following standards apply to the System Values settings related to security functions:

- QSECURITY = 30 (Password and Object Level Security).
- QCRTAUT = \*use.
- QDSCJOBITV = 30.
- QDSPSGNINF = 1.
- QINACTITV = 30.
- QINACTMSGQ = \*DSCJOB.
- QLMTDVSSN = 0.
- QLMTSECOFR = 0.
- QMAXSGNACN = 2.
- QMAXSIGN = 3.
- QRMTSIGN = \*FRCSIGNON.

- QUSEADPAUT = \*yes.  
QALWOBJRST = \*NONE.

### B.3 User Accounts

Limit command capabilities as appropriate.

- Special Authorities shall be given careful consideration before being distributed.
  - \*ALLOBJ
  - \*SECADM
  - \*JOBCTL
  - \*SPLCTL
  - \*SAVSYS
  - \*SERVICE
  - \*AUDIT
  - \*IOSYSCFG

### B.4 Configure Profile Security

- All IBM shipped profiles (i.e. QSECOFR and Dedicated Service Tools (DST)) are shipped with passwords of the same name. The password shall be changed immediately after installation.
- I.S. Technical Support Group
- I.S. Programmers
- I.S. Operator
- I.S. Help Desk
- I.S. Network Administrator
- Application User
- Common Profiles
- Communication Connections Profiles

## ADDENDUM C

### UNIX OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

#### UNIX SECURITY

The following information provides an overview of current known risks and vulnerabilities that need to be addressed to provide a standard level of information security controls for Tenet information assets. Individual Administrators shall use system specific resources to obtain and customize information security checklists to accomplish this goal.

##### C.1 Protect the System from Undesirable Booting

The boot up process and bootable drives can be used to circumvent the operating system. When practical:

- The boot sequence shall not use removable media (CDROM, TAPE, or FLOPPY).
- Ensure that the final run state will be multi-User and multi-tasking (usually init state 2 or 3).
- When there are troubles in booting to multi-User, require a password to gain access to single User mode and root access.
- Do not allow the system to stop in "interactive/firmware" mode.
- Primary boot shall from the boot partition of disk 0 (if it is different, it shall be documented).
- Disable network booting.
- Document disk(s) and file systems.
- Have two disks that contain the critical file systems and boot block. These can easily be kept in sync and used to bring the system up easily during a disk failure.
- Document the disk numbers and file system partitions for all file systems.
- Many systems have a special key sequence to halt a system. This shall be disabled on servers.
- Servers shall restrict root login to the console. Remote access can be gained by a login as a normal User and using the su/sudo/sur command.
- Install, configure, and use third party products that monitor the system configuration and boot files.

## C.2 User Accounts

The following guidelines shall be followed when creating UserIDs:

- Create accounts with unique UserID.
- UID 0 shall be assigned to root only.
- Default PATH variable shall have 'system' directories first and '.' last.
- Default UMASK of 022 shall be adhered to.

## C.3 Password Management

The following guidelines shall be followed for User and group accounts.

- Where possible the 'shadow' file shall be utilized.
- Password advisor functions shall be performed.
  - If the operating system is not capable of performing these functions, administrators shall investigate and implement third party software to enhance the password process.

## C.4 Managing Root Access

The root account shall only be accessible by the Unix Administrators.

- The number of individuals with the root password shall be minimized.
- Direct access to the root account shall be allowed only at the system console.
- System Administrators needing root access shall use the 'sur' program.
- The root login environment shall contain the following controls:
  - The default PATH shall not contain '.' or the current working directory.
  - The default PATH shall not contain any "world writable" directory. (777).
  - The .exrc file shall not be enabled.
  - If .rhosts file exists, permissions shall be 400, and owned by root.
  - Root home directory shall be owned by root and read/write only by root.

- Administrators shall consider changing the root password more frequently than standard passwords, 30 days is suggested. Whenever a team member leaves, this password shall be changed.
- For instances where Users other than administrators may need root access, the ‘sudo’ command shall be used. Users shall be given this access on a single command basis.

#### C.5 NFS/NIS

If implemented, this will be used for local trusted hosts only.

#### C.6 Auditing

- A program that has the setuid() or setgid() set, and is owned by root, or another ‘system’ account, shall be monitored on a daily basis.
  - At least weekly, a check shall be made to add any new programs to this audit. The audit shall include at least the Date/time stamp, Checksum, and Size of file.
  - Any change to these files shall be immediately reported as per the Incident Handling Policy 4.0.0 and its associated Standard and procedures.
- The location and name of system configuration files varies with the different Unix variants. The system configuration files shall be monitored, daily, for unexpected changes. A short list of those files includes:
  - /etc/hosts
  - /etc/passwd (and the shadow file where it exists.)
  - /etc/services
  - /etc/inetd.conf
  - /etc/inittab
  - /etc/profile
  - This list shall be expanded depending on system requirements.

#### C.7 File/Directory Permissions

The following general guidelines shall be followed where applicable.

- Where possible, directories shall not have “world” write permission, or 777.

- If that is not possible, then permission shall be set to 177, to allow only the custodian to remove files in that directory.
- If they exist, .rhosts or .netrc files shall be read/writable by the custodian only.
- Shell scripts that are run by root shall not have world write access.
- Directories that are included in the PATH variable shall not have world write access.

## C.8 Proactive Monitoring

There are several different public domain packages available to monitor system agent activities. Any of these packages, along with “home grown” programs can be used to monitor system agents. A short list of those agents might be:

- telnetd
- ftpd
- inetd
- snmp
- tftp
- sendmail (Particular attention shall be made to attempt to secure sendmail.)
- smb
- imap