



|   |  |                                 |                           |
|---|--|---------------------------------|---------------------------|
|  | <b>Information Privacy and Security Program</b>                |                                 | <b>No. EC.PS.04.09</b>    |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b>                    | <b>1 of 7</b>             |
|   |  | <b>Effective Date:</b>          | <b>10-27-16</b>           |
|   |  | <b>Retires Policy Dated:</b>    | <b>09-16-13</b>           |
|   |  | <b>Previous Versions Dated:</b> | <b>12-22-04, 11-06-00</b> |

## I. PURPOSE:

The purpose of this standard is to provide direction for administration and maintenance of operating system security for Tenet information assets.

## II. DEFINITIONS:

- A. **“Administrators”** means the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.
  - B. **“AS/400”** or **“Application System/400”** refers to IBM's midrange business computer system platform for business applications
  - C. **“Confidential Information”** shall have the same meaning as Proprietary Information.
  - D. **“Proprietary Information”** means any trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, customer, patient, employee, investor, or business information, whether in oral, written, graphic or electronic form.
  - E. **“UNIX”, “LINUX”** or **“X-NIX”** refers to a family of multitasking, multiuser computer operating systems that derive their base from the original 1970's AT&T UNIX operating system.
  - F. A **“User”** means an individual that inputs/outputs data to/from Tenet information assets. These individuals are collectively referred to as Users, and may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, business partners and electronic (web site) visitors.
  - G. **“Windows Server”** refers to a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications.
  - H. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.
-


|   |  |   |
|---|--|---|
|  | <b>Information Privacy and Security Program</b>                | <b>No. EC.PS.04.09</b>                        |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b> 2 of 7                           |
|   |  | <b>Effective Date:</b> 10-27-17               |
|   |  | <b>Retires Policy Dated:</b> 09-16-13         |
|   |  | <b>Previous Versions Dated:</b> 12-22-04, 11- |

### III. STANDARD

Information Systems Administrators and other individuals must apply these standards to ensure a consistent level of information security across Tenet information assets.

#### A. Naming Standards

1. Regardless of physical, virtual, single-instance, multi-instance, or multi-tenancy state, each active software instance must be able to be uniquely identified for non-repudiation purposes.
2. Distributed software must use a centralized directory service account management system, such as Active Directory, for operation system authentication where able to be configured.
3. Each software instance communicating with other distributed devices must use network hostnames label that are distinguishable within the enterprise and conform to the syntax and character limitations of the protocol being used. For internet protocol (IP)-based communications, the hostname label conformance and limitations are specified in the combination IETF RFC 1035, IETF RFC 1912, subsequent RFC. [Hostnames cannot exceed 63 ASCII characters and may use any ASCII letters, digits, plus the '-' character, but start and end only with a letter or digit].
4. Each operating software instance or centralized directory service account management system may place additional restrictions on hostname labels. Hostname labels used with Active Directory or requiring backwards compatibility with NetBIOS devices will be restricted to 15 ASCII characters length.
5. The Naming Convention guideline for servers is the following:  
Windows Server or Active Directory joined system.
  1. AAA=COMPANY (TEN=TENET)
  2. BBB=FACILITY (TSC=TENET SERVICE CENTER)
  3. CCC=PRIMARY ACTIVE DIRECTORY DOMAIN

|   |  |                                 |                      |
|---|--|---------------------------------|----------------------|
|  | <b>Information Privacy and Security Program</b>                | <b>No.</b>                      | <b>EC.PS.04.09</b>   |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b>                    | <b>3 of 7</b>        |
|   |  | <b>Effective Date:</b>          | <b>10-27-17</b>      |
|   |  | <b>Retires Policy Dated:</b>    | <b>09-16-13</b>      |
|   |  | <b>Previous Versions Dated:</b> | <b>12-22-04, 11-</b> |

Example: TH=Tenethealth  
MT-Model  
ER=eRoot

4. DDDDDDD=PRIMARY APPLICATION AND UNIQUE PURPOSE. Inclusive of any operation system (W12=WINDOWS 2012), and server number (01-SERVER 01).

Example = TENHDCPTHDC08-01 is a Tenet asset (TEN) at Headquarters Datacenter (HDC) on the Tenethealth domain (TH) primary application of domain services (DC) running Windows Server 2008 (08) uniquely identified as Server #1 (-01)

Non-Active Directory joined device, usually a non-Windows standalone device


- a. AAA=COMPANY (TEN=TENET)
- b. BBB=FACILITY (TSC-TENET SERVICE CENTER0
- c. CCC=OPERATING SYSTEM OR PRIMARY APPLICATION (ESX=VMware ESX)

DDDDDDDDDD=OPERATING SYSTEM OR PRIMARY APPLICATION (ESX=VMware ESX)Example = TENDBKPKIHSM01 is a Tenet asset (TEN) at Databank Datacenter (DBK) primary application of private key infrastructure (PKI) running Hardware Security Module (HSM) uniquely identified as #1 (01)

## B. Administration

Administrators must:

1. Consider security impacts and configurations in the beginning of the system design process.
2. For new implementations or changing the architecture of existing systems, follow EC.PS.04.05 Technical Controls Security Standard to obtain approval from the Information Security Officer and the Corporate Information Security Department before establishing new servers.
3. Per EC.PS.04.04 Activity Logs and User Monitoring Standard, configure assets so that no single person can make an error or manipulate the records without such events being detected.
4. Use and support standard naming conventions for UserID codes (see EC.PS.04.05 Technical Controls Security Standard), production program

|   |  |   |
|---|--|---|
|  | <b>Information Privacy and Security Program</b>                | <b>No. EC.PS.04.09</b>                        |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b> 4 of 7                           |
|   |  | <b>Effective Date:</b> 10-27-17               |
|   |  | <b>Retires Policy Dated:</b> 09-16-13         |
|   |  | <b>Previous Versions Dated:</b> 12-22-04, 11- |


names, production file names, and system names.

5. For the cardholder data environment implement only one primary function per server (virtual or otherwise).
6. Administrators must follow change management processes in accordance with EC.PS.04.04 Technical Controls Security Standard.
7. Maintain the operating system configuration.
  - a. Ensure each system is configured with industry accepted and Tenet approved hardening standards.
    - i. Update the documented hardening standard as new vulnerabilities are identified.
  - b. Enable only the necessary services.
  - c. Apply security patches provided by operating system vendors per current Tenet Patch Management Standards.
  - d. Monitor resources to identify newly released information about threats and vulnerabilities per the IS.PRO.04.09 Vulnerability Assessment Remediation Procedure.
  - e. Upgrade the version of the operating system when appropriate.
8. Users must be configured to perform their work through a series of menus or icons to restrict access to the operating system commands.
9. Perform regular preventive maintenance on all information assets.
  - a. Repairs and servicing of equipment must be performed only by authorized maintenance personnel.
  - b. Preventive maintenance must be performed at the vendor's recommended service intervals and maintenance specifications.

**C. Access to Utilities**

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

**D. Access to Broadcast Tools**

|   |  |   |
|---|--|---|
|  | <b>Information Privacy and Security Program</b>                | <b>No. EC.PS.04.09</b>                        |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b> 5 of 7                           |
|   |  | <b>Effective Date:</b> 10-27-17               |
|   |  | <b>Retires Policy Dated:</b> 09-16-13         |
|   |  | <b>Previous Versions Dated:</b> 12-22-04, 11- |

Broadcast tools found in computer asset operating systems, e-mail systems, voice mail systems, and others, must only be used by system Administrators or with Tenet Entity Information Security Officer approval.

E. Last Logon Time and Date

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

F. System Logoff

All logoff procedures must 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 Attachments provide guidelines for the configuration and maintenance of operating systems. Administrators must 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. Refer to the following attachments:


1. Attachment A: Windows Administrative Procedure
2. Attachment B: AS/400 Administrative Procedure
3. Attachment C: Unix Administrative Procedure

#### IV. IMPLEMENTATION:

A. Information Privacy and Security Program

1. Tenet Facilities

- a. The Privacy and Security Compliance Officer, Tenet Facility Information Security Officer, Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of Program Standards at the facility level.
- b. Tenet Facility Leadership, in coordination with the Privacy and Security Compliance Officer and Tenet Facility Compliance

|   |  |   |
|---|--|---|
|  | <b>Information Privacy and Security Program</b>                | <b>No. EC.PS.04.09</b>                        |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page:</b> 6 of 7                           |
|   |  | <b>Effective Date:</b> 10-27-17               |
|   |  | <b>Retires Policy Dated:</b> 09-16-13         |
|   |  | <b>Previous Versions Dated:</b> 12-22-04, 11- |

Committee will create specific policies and procedures as necessary in order for the Tenet Facility to operationalize the Program.

- c. Tenet Facility Leadership will report Program monitoring activity to the Privacy and Security Compliance Officer.


2. Corporate Office (Dallas/Nashville)/ Market

- a. Tenet's Information Privacy/Security Office will work with the Privacy & Security Compliance Officers, Tenet Facility PIRTS, Tenet Facility Information Security Officers Tenet Facility Compliance Committees, and Tenet Facility Leadership to develop, maintain, and update policies, procedures and standards for protecting the privacy of PHI, PII, PCI cardholder data and other Confidential/Proprietary Information affording patients their rights with respect to their PHI, PII, PCI cardholder data.
- b. Tenet Corporate and Tenet Facilities must incorporate these standards into their specific policies and procedures where necessary.

- 1.

## V. REFERENCES:

- EC.PS.01.00 Information Privacy and Security Administration Policy
- EC.PS.04.00 Information Security Policy
- EC.PS.04.02 User Security and Conduct Standard
- EC.PS.04.04 Activity Logs and User Monitoring Standard
- EC.PS.04.05 Technical Controls Security Standard
- IS.PRO.04.09 Vulnerability Assessment Remediation Procedure
- Information Privacy & Security Glossary of Definitions
- NTT Data Services Procedure: Tenet Standard Firewall Operations
- NTT Data Services Procedure: Tenet Standard Network Devices Configuration
- NTT Data Services Reference: Tenet Standard Infrastructure Application Delivery Controller

|   |  |   |
|---|--|---|
|  | <b>Information Privacy and Security Program</b>                | <b>No. EC.PS.04.09</b>                        |
|   | <b>Title:</b><br><br><b>OPERATING SYSTEM SECURITY STANDARD</b> | <b>Page: 7 of 7</b>                           |
|   |  | <b>Effective Date: 10-27-17</b>               |
|   |  | <b>Retires Policy Dated: 09-16-13</b>         |
|   |  | <b>Previous Versions Dated: 12-22-04, 11-</b> |

Operations Procedure

## VI. ATTACHMENTS:

- Attachment A: Windows Administrative Procedure
- Attachment B: AS/400 Administrative Procedure
- Attachment C: Unix Administrative Procedure

## 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”.
- Set a BIOS password.
- Set remote access card password (physical)

#### A.2 File System

FAT partitions shall be used for key boot files boot.ini, ntldr, ntdetect.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 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



## WINDOWS OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

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 EC.PS.04.05 Technical Controls Security Standard 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 EC.PS.04.02 User Security and Conduct Standard for further information.
- 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 or better.
- Secure the event log.
- Enable audits of backups and restores.
- Manage log files, see EC.PS.04.04 Activity Logs and User Monitoring Standard for further details on this subject.

### A.4 User Accounts and Password Restrictions

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

- EC.PS.04.05 Technical Controls Security Standard
- EC.PS.04.02 User Security and Conduct Standard
- Default Administrator Account:
  - o Must rename or disable the account
  - o Restrict distribution.
  - 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

## WINDOWS OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

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 Windows machines have their guest account disabled, regardless of the machine's function. (Group policy)

### A.5 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.6 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.7 Install latest version of Tenet approved Antivirus software

### A.8 Install latest version of Tenet approved Encryption; both Full Disk and Media.

## **WINDOWS OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS**

- Be sure the server is reporting to the EPO server.

### **A.9 Install Tenet approved systems management product.**

For each system

- Be sure to install Tenet approved systems management product and/or agent on server to ensure proper inventory and security.

### **A.10 Network**

For each system

- Name each NIC (Network Interface Card) for its function.
- Uncheck “Allow Computer to turn off this device to save Power”.
- Disable all unused NICs.
- Disable IPV6 for each card.

## 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.
- QDSCJOBTV = 30.
- QDSPSGNINF = 1.
- QINACTTV = 30.
- QINACTMSGQ = \*DSCJOB.
- QLMTDVSSN = 0.
- QLMTSECOFR = 0.
- QMAXSGNACN = 2.
- QMAXSIGN = 3.
- QRMTSIGN = \*FRCSIGNON.
- QUSEADPAUT = \*yes.

## **A/S 400 OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS**

- 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

## 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.
- For physical servers/ bare-metal installation, 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 and predefined hosts only. In general, 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.

## **UNIX OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS**

### **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 may be allowed only at the system console and predefined hosts.
- System Administrators needing root access shall use the 'sudo' 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

## UNIX OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS

root.

- Administrators shall consider changing the root password more frequently than standard passwords. This must be changed at least once every 90 days. 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



## **UNIX OPERATING SYSTEM CONFIGURATION RECOMMENDATIONS**

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.