	Information Systems Procedure	No.	IS.PRO.04.06	
	PATCH MANAGEMENT PROCEDURE	Title:	Page:	1 of 8
		Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

I. PURPOSE:


The purpose of this procedure is to detail and standardize the patch management process, time frames, activities, and reporting for Tenet Entities as it applies to all Tenet-owned computing assets. This procedure provides technical standards for managing Operating System and Application patches for review, deployment, and verification for Tenet information systems.

II. DEFINITIONS:

- A. An “**FDA Device**” – devices that have patching restrictions dependent on FDA approval.
- B. “**Systems Management**” – the service Provider endpoint management and deployment team.
- C. A “**Patch**” – a product update to provide an enhancement or correct vulnerability for an operating system or application.
- D. A “**Patch Management Coordinator**” or “**Service Provider Lead**” – the Service Provider Information Security Team Lead responsible for coordination functions.
- E. A “**Patch Management Lead**” or “**Tenet Lead**” – the Corporate Information Security Team Lead responsible for direction and lead functions.
- F. A “**Patch Management Team**” –” – the Service Provider Team responsible for performing the patch management functions.
- G. A “**Server**” – a device running a Server Operating System or other devices acting as Servers.
- H. A “**Workstation**” – a desktop, laptop, tablet, or thin client.

III. PROCEDURE:

- A. Workstation Patch Management Procedure
 - 1. Vendors typically release patches on the second Tuesday of each month. The Systems Management team will download the patches on the second Wednesday of each month.
 - 2. The Systems Management Team will replicate the patches to the standard software replication shares by the second Thursday of each month.
 - 3. The Tenet Lead will provide the approved patch list by the second Thursday of each month to the Service Provider Lead.


	Information Systems Procedure	No.	IS.PRO.04.06	
	Title:	Page:	2 of 8	
	PATCH MANAGEMENT PROCEDURE	Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

4. The Service Provider Lead will coordinate with the Systems Management Team to deploy the approved patches to the pre-identified Pilot test user workstations across Tenet as defined in Section III.C.1. Patch Assessment.
5. The Systems Management Team will review feedback from patch testing and share any reported issues with the Tenet Lead. The Tenet lead will review any testing issues with the affected application owners for direction.
6. The Tenet Lead will issue an approval to complete the enterprise workstation patch Deployment with any necessary exceptions.
7. The Systems Management Team will deploy the patches to the enterprise workstations completing the patch management process.
8. The local Information Services team must configure workstations to perform an auto-reboot process on a weekly basis to ensure patches are fully applied.

B. Server Patch Management Procedure

NOTE: Tenet Security requires that servers receive current security patches within 14 days of release.

1. Working with the Server Support team and Applications owner for the hosted applications, the Service Provider Lead will create a list of affected servers and the corresponding patch schedule.
2. The Service Provider Lead will create a Patch Management workbook to document the affected servers and applications and their patch dependencies (*e.g.*, Cerner Patch release process), and coordinate a schedule for application patching and rebooting of the affected servers with the Server Administration Team.
3. After reviewing the schedule, the Server Administration Team will separate the affected systems into Auto-Reboot and Manual Reboot Groups. The Server Administration Team will provide the list to the Service Provider Lead.
4. The Service Provider Lead will coordinate and submit a Change Management (CM) request with the complete reboot schedule and provide the corresponding CM ticket to the Systems Management Team for deployment.
5. To minimize production disruption, the Server Administration Team must deploy server patches to Test and Model environment servers prior to

	Information Systems Procedure	No. IS.PRO.04.06	
	PATCH MANAGEMENT PROCEDURE	Title:	Page: 3 of 8
			Effective Date: 12-26-18
			Retires Procedure Dated: 05-16-16
			Previous Versions Dated: 06-29-17

production systems.

6. As the Server Support team implements new servers, they will submit updates to the appropriate patch groupings.

The following is an example of a general patch management schedule.

**General Patch Management
Timeline July 2015**


Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1 Scheduled Hospital Weekly Reboot *	2	3	4
5	6	7	8 Scheduled Hospital Weekly Reboot	9	10	11
12	13	14 Vendor Patch Release Tenet Review	15 Patches loaded in Patch Mgmt. Sys Scheduled Hospital Weekly Reboot	16 Tenet Approves Patch list Deploy patches to IS Test Group	17 Deploy patches to Apps Test Group	18
19	20 Patch Testing	21 Patch Testing	22 Patch Testing and Scheduled Hospital Weekly Reboot	23 Patch Testing	24 Patch Testing	25 Server Patch Groups Start – Scheduled
26	27 Approval to Deploy	28 Full Patch Deployment	29 Scheduled Hospital Weekly Reboot	30	31	1
2	3	4 PACS Patch Deployment	5 Scheduled Hospital Weekly Reboot	6	7	8

***NOTE:** Weekly reboots are for workstations only

C. Patch Assessment

The Tenet Lead will approve all patches and/or exceptions.

1. Patch Review – The Tenet Lead will review vendor patch-release information for operating systems and common business applications and recommend patches for deployment. The Tenet Lead will review and approve patches for testing and for final deployment.

	Information Systems Procedure	No.	IS.PRO.04.06	
	PATCH MANAGEMENT PROCEDURE	Title:	Page:	4 of 8
		Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

2. Preliminary Approval – The Tenet Lead will identify patches that may have adverse effects that should be included in testing for that month’s patch cycle and notify the Systems Management Team to distribute patches to the respective test group devices for testing. This is typically 48-72 hours after patch release by the vendor.
3. E-mail notifications – The Tenet Lead will complete notification for O/S systems and application patches that have been identified for patch upgrade. The e-mail must include the 7-day testing window and, if no issues are experienced on the test systems, the patches will be deployed to the rest of the enterprise 8 days from the receipt of the e-mail notification.

NOTE: Patch testers are responsible for notifying the Systems Management team of any technical issues encountered during testing.


D. Patch Evaluation

Patch testing must be completed on a subset of systems or applications identified by the regions and application owners.

1. Every Tenet Entity should maintain a minimum of two test workstations configured with the major applications used by that entity and two Technical workstations.
2. Additionally, application support and central infrastructure teams should identify workstations for preliminary patch testing for centrally managed applications and infrastructure control systems. The Tenet Entity will provide these workstation names to the Systems Management team. The Systems Management team will maintain a list of patch testing devices separated by group as indicated in the Workstation Patch Management Procedure.
3. Hospital Information Services Teams are responsible for executing the patching, but the application owners are accountable for testing their applications.
4. The testing team must report any issues to the Service Provider Lead for further review and evaluation. The Service Provider Lead will present a compiled issues report to the Tenet Lead for final review and approval of deployment.

E. Patch Deployment

Upon completion of the testing process, the Tenet Lead will release approved patches for deployment.

	Information Systems Procedure	No.	IS.PRO.04.06	
	PATCH MANAGEMENT PROCEDURE	Title:	Page:	5 of 8
		Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

1. Patching Notification – A notification e-mail must be sent out to the enterprise briefly describing the new patches being released and the reboot requirements for the affected workstation.


NOTE: Please review Appendix A for an example e-mail notification.

2. Patch Deployment – The patch updates will be deployed to the remaining workstations excluding approved exceptions in exempted and special patch groups.
3. Reboot Alerts – Weekly forced workstation reboots will be deployed per entity upon completion of the patch management configuration. These are currently scheduled for early Wednesday mornings at 2:00 AM for the majority of enterprise workstations, excluding a small number of device exceptions.
4. During the Server Patching Workbook review, the Tenet and Service Provider Leads will determine the server reboot cycle.

F. Roles

This section covers the specific roles that certain individuals have regarding patch management.

1. Patch Management Lead (Tenet Lead)
 - a. Tenet Information Security will perform the overall patch management lead functions.
 - b. The Patch Management Lead reviews and approves all patches recommended by the Patch Management Coordinator. Once reviewed, the Patch Management Lead will provide approval to send out the e-mail notifications and continue the normal patching process.
 - c. The Patch Management Lead will review any applications that have cumulative patches requiring testing before issuing approval to continue the normal process. Some examples include: Internet Explorer involving Active X patches, Java patches, Adobe patches, etc.
2. Patch Management Coordinator (Service Provider Lead)
 - a. Service Provider Information Security will perform the patch management coordination functions.

	Information Systems Procedure	No.	IS.PRO.04.06	
	Title:	Page:	6 of 8	
	PATCH MANAGEMENT PROCEDURE	Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

b. The Patch Management Coordinator prepares the initial vendor patch listing and notifications for the Patch Management Lead to review.

c. The Patch Management Coordinator will review patches identified for testing and communicate approval to proceed with testing and final deployment upon receipt of approvals from the Patch Management Lead.

3. Patch Management Team (Systems Management Team)

a. Service Provider Systems Management Team will perform the patch management deployment functions.

b. The Patch Management Team will complete loading of patches into the patch management system; distribution of patches for testing, distribution of approved patches, and reporting for these activities.

c. The Patch Management Team will participate in technical review of patches as required.


G. Patch Exclusion Groups

Patch Exclusion groups are groups of endpoint devices that cannot be patched on the same schedule as other endpoint devices. These devices are usually patched through alternate patch systems, manually or other mechanisms. The preferred mechanism for managing exclusion groups is by creating Active Directory (AD) Organizational Units (OU) or managed by the current endpoint management system. Any entity systems not currently managed within AD must be managed by the endpoint management system.

1. Patch Exclusions – These are un-deployed vendor-released patches not for various reasons, e.g. causing vulnerabilities, corrupt patches, compatibility issues, etc. Application owners are responsible for ensuring compliance on devices that run their application.

H. Patching for Excluded Devices

1. There are instances where workstations may not be patched due to vendor support or other restrictions. Example: Workstations used with special devices (e.g., Biomedical devices, FDA devices, etc.). In these cases, the Tenet Entity should request an exception from the Corporate Information Security Team and clearly define the process and the mitigating controls

	Information Systems Procedure	No.	IS.PRO.04.06	
	Title:	Page:	7 of 8	
	PATCH MANAGEMENT PROCEDURE	Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

to limit information security risks associated with these devices. For example, manual patching of devices based on vendor-approved patches with some form of network isolation would be an appropriate mitigation of risk for these device types.

2. Although a Tenet Entity may have received an approved exclusion for standard patch management of a particular device, the Tenet Entity is responsible for patch compliance of that device by detailed monthly review and application of approved patches for the affected device.
3. Hospital Information Services is responsible for executing the patching, and the application owners are accountable for testing the effects of the installed patches on their respective applications.
4. Hospital Information Services will group excluded workstations for patch management. They will add them to a custom deployment schedule. For example, PACs/CPACs workstations follow a uniform patch release schedule in coordination with the McKesson vendor.

I. Patching Scope

1. Operating Systems: Microsoft supported operating systems only; other operating systems would be best effort.
2. Vendors in Scope: Microsoft (all Severity levels), Adobe, Oracle (Java), other Browser, common business applications and third party supported vendor patches.

J. Reporting and Compliance


IT Compliance reports exist in the patch management system to track patching success and overall workstation IT compliance with Tenet Standard Information Security tools and patching.

K. Responsible Party

The Tenet Entity Information Services Director (ISD) is responsible for ensuring that all personnel adhere to the requirements of this policy. The ISD ensures adoption and implementation of these practices at their respective Entity, and that instances of non-compliance with this policy are reported to the Corporate Information Security Team.

L. Auditing and Monitoring

Patch management effectiveness is reflected in the entity level vulnerability reports. Service Provider and Tenet leadership review these reports in the monthly

	Information Systems Procedure	No.	IS.PRO.04.06	
	Title:	Page:	8 of 8	
	PATCH MANAGEMENT PROCEDURE	Effective Date:	12-26-18	
		Retires Procedure Dated:	05-16-16	
		Previous Versions Dated:	06-29-17	

Hospital Information Services (HIS) Scorecards.

M. Exceptions

Exceptions to this procedure must be documented and submitted for approval through the Corporate Information Security and Compliance Exception process. All exceptions are reviewed annually by the Corporate Information Security Team.

IV. REFERENCES:

- 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
- EC.PS.04.06 Application Security Standard
- IS.PRO.04.00 Tenet Asset Security Requirements

Appendix A

Example Patching Notification Email

From: Tenet WSUS Admin Team
Sent: Monday, June 01, 2015 12:52 PM
To: DL-WSUS-FacilityAdministratorNotification@tenethealth.com
Cc: Vega, Ruben <Ruben_Vega@Dell.com>
Subject: June 2015 Microsoft Update Approvals -Facilities

Dell - Internal Use - Confidential

The updates listed below were released or revised since our last patch window. The Tenet WSUS Admin Team will be approving these updates for availability to all Tenet hospitals/facilities on **Tuesday, June 15th 2015**.

Bulletin ID	Bulletin Title and Executive Summary	Maximum Severity Rating and Vulnerability Impact	Restart Requirement	Known Issues	Affected Software
MS15-043	Cumulative Security Update for Internet Explorer (3049563) This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.	Critical Remote Code Execution	Requires restart	-----	Microsoft Windows, Internet Explorer
MS15-044	Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110) This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync, and Microsoft Silverlight. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains embedded TrueType fonts.	Critical Remote Code Execution	May require restart	3057110	Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Microsoft Lync, Microsoft Silverlight
MS15-045	Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002) This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.	Critical Remote Code Execution	May require restart	-----	Microsoft Windows

Tenet WSUS Admin Team
 tenet infrastructure security - tenet account

Dell | Services

TenetWSUS-admin.psc@ps.net

NAME	ENTITY TYPE	FACILITY.ROLL-UP	DIVISION	REGION	STREET ADDRESS	ADDR FOR SORTING	CITY	ST	ZIP
TEN-FRM-South Campus	OTH	SS-FRM	TEN-HospAMB	Southern States	1 3rd Ave NW	3rd Ave	Hickory	NC	75088
TEN-SSPS-CAR-Riverside Wmms Care #3	PhyOfc	SS-HHH	TEN-PhyOfc	Southern States	1 Burnt Church Rd	Burnt Church Rd	Bluffton	SC	1605
TEN-PAPS-HAH 1 Commerce Blvd Ste 103 Neuro Surgery	PhyOfc	NEAMB-HabPA	TEN-PhyOfc	Northeast	1 Commerce Blvd Ste 103	Commerce Blvd	Philadelphia	PA	70809
TENNM-NEPS-SVMG-Eaton Pl-Ste 22	PhyOfc	NEAMB via Incidents in CareTech tool	TEN-PhyOfc	Northeast	1 Eaton Pl Ste 22	Eaton Pl	Worcester	MA	29732
TENNM-NEPS-SVMG-Eaton Pl-Ste 23	PhyOfc	NE-SVH via Incidents in CareTech tool	TEN-PhyOfc	Northeast	1 Eaton Pl Ste 23	Eaton Pl	Worcester	MA	33334
TENNM-NEPS-Cancer & Wellness Ctr	OTH	NE-SVH	TEN-HospAMB	Northeast	1 Eaton Pl Ste 100	Eaton Pl	Worcester	MA	33410
TENNM-NEPS-W Surburban FamMed	OTH	NEAMB-IL	TEN-HospAMB	Northeast	1 Erie Ct Ste 6160	Erie Ct	Oak Park	IL	34242
TENNM-NEPS-W Sub Pto Ofc BldOrtho	PhyOfc	NEAMB-IL	TEN-PhyOfc	Northeast	1 Erie Ct Ste 7010	Erie Ct	Oak Park	IL	33143
TENNM-NEPS-MWVG-East Main St	PhyOfc	NEAMB via Incidents in CareTech tool	TEN-PhyOfc	Northeast	1 Main St E Ste 208	Main St E	Northborough	MA	34972
TEN-FLPS-TFPS-100 NW 170 St Ste 206	PhyOfc	FLPS	TEN-PhyOfc	Florida	100 170 St NW Ste 206	170 St NW	North Miami Beach	FL	34957