UNM HEALTH SCIENCES CENTER

Applies To: **All HSC Workforce Members**
Responsible Department: **Information Technology**
Revised: **New**

Title: **HSC IT Security Patching**	**Standard**

DESCRIPTION/SCOPE

This standard establishes processes and guidelines for the security patching of IT systems at the Health Sciences Center (HSC). The standard applies to operating systems and applications running on HSC servers, and computers as defined by the HSC computer inventory standard. It is intended that critical security patches will be applied immediately or as promptly as possible. Non-critical patching will be applied at the earliest opportunity as indicated within the patching standards described below.

The overall strategy of the HSC is to have consolidated and coordinated patching solutions that address common operating system and application needs.

This HSC patching standard includes all health care components of UNM that are under the jurisdiction of the HSC as designated in UNM Board of Regents Policy 3.4 and UNM Board of Regents Policy 3.7.

REFERENCES

The patching standard supports compliance with the HIPAA Security Rule through the implementation of HSC level Security Policies, including but not limited to: HSC-300 ePHI Security Compliance, HSC-220 Information Access and Security, HSC-210 Security of HSC Electronic Information, and HSC-210.1 Baseline IT Security Procedures.

DEFINITIONS

A security patch is a piece of software that is applied to an operating system or application to fix a security vulnerability. Vulnerabilities are weakness in computer code that can be exploited by an attacker using malware such as a virus or a web site that has hidden code. Attackers may gain control or access to computer processes or data. Attacks typically exploit vulnerabilities for which patches have long been available, but not been applied. To assist with deployment priorities, security patches may be rated as; Critical, High (Important), Medium (Moderate) or Low severity.

For purposes of this standard, any reference to applying patches means the patch has been loaded on the system and the patch has been activated (often by a system re-boot).

PATCHING STANDARDS

1. Patching Levels

1.1. Critical Systems:

System owners may define a system as critical in addition to using the criteria defined in Policy HSC-300 based on the following:

a) Servers containing ePHI, confidential or other sensitive data.

DRAFT

b) Workstations containing ePHI or other confidential, sensitive or business data that is subject to specific UNM/HSC policy requirements for security.
c) Infrastructure systems and devices providing critical services required by HSC information systems (e.g., DNS/DHCP).

For Critical Systems the compliance target for critical and high OS and application security patches is that 95 percent are applied within 30 days of the release by the vendor, excluding documented exceptions.

1.2. Non Critical Systems:

Security patches are applied according to device classification standards created and maintained by IT service units, such as: office computer, conference room devices, public computing devices, lab or exam devices, etc. These devices are subject to the following:

a) All systems must meet minimum patching standards established by IT units based on device classification for non-critical systems. If no standards are defined, devices are to be treated as "critical" and patched to standards for critical systems.
b) Servers are to be patched as critical systems with exceptions documented through Help.HSC by system owners and approved by IT security.

For non-critical systems the compliance target for critical and high OS and application security patches is that 80 percent or higher are installed within 60 days of release from the vendor, excluding documented exceptions (See "Exception Processes" below).

1.3. If a system cannot be patched in compliance with this standard a Help.HSC ticket must be submitted with the reason. Only exceptions approved through Help.HSC will be excluded from patching requirements.

2. Patching Tools

2.1. UNMH IT and HSLIC IT provide centralized tools for patching supported HSC operating systems and applications. Patching tools include but are not limited to; WSUS, SCCM, Shavlik (3rd party patching), Secunia (student use), etc. Patching tools may change without notice.

2.2. Departments or units are responsible for patching any operating system or application that is unique to the respective department or unit.

2.3. For HSC supported operating systems and applications, departments or units are required to use centralized patching tools as defined by UNMH and HSLIC unless approved by the Information Security Office for a stand-alone solution. If at any time systems fall below HSC IT Security Council goals for patching, the systems will be subject to a conversion to HSC centralized patching services.

2.4. To support a centralized patching strategy, devices connected to the HSC network will be required to permit patching tools access to evaluate and patch operating system and applications as appropriate to the respective device classification. Exceptions must be handled through an approval process recorded in the Help.HSC system.

2.5. Patching tools used outside of the centralized patching tools must be documented by the system owner, and verified by an IT security analyst for effectiveness as determined by an IT Security review.

3. Exception Processes

DRAFT

3.1. HSC-wide exceptions to this HSC Patching Standard will be documented according to a process established by UNMH IT and/or HSLIC IT for known IT security vulnerabilities when a patch is not released.
3.2. Individual patching exceptions will be submitted through Help.HSC and reviewed by UNMH and/or HSLIC IT Security staff who will maintain a list of approved exceptions.
3.3. Any approved exception is required to have documented mitigation controls for critical systems and any high risk vulnerabilities. Mitigation controls must be reviewed by an IT Security Analyst through the Help.HSC system and approved as defined by procedures within Help.HSC. If no mitigation is possible, the exception must still be reviewed by an IT Security Analyst through the Help.HSC system and approved as defined by procedures within Help.HSC.
3.4. Each IT unit will maintain a list of exceptions approved through Help.HSC procedures. At least annually the list will be reviewed by system owners to determine if the exception is still needed and up update mitigation controls if needed.

4. Patching Validation and Verification

4.1. Tools, such as Nessus, Nexpose, etc., are used to scan the network for security vulnerabilities. Network security scans may be performed periodically and randomly by authorized IT staff. The HSC IT Security Council will review and approve all IT staff authorizations for scanning across organizations.
4.2. Systems may be scanned for patch compliance from a central console using credentials authorized by the HSC Information Security Officer. Any system that does not allow credentialed scanning must have an exception approved through a Help.HSC ticket. Those systems exempted from a credentialed scan will undergo a non-credentialed scan following the same procedures as a credentialed scan and may be subject to additional requirements.
4.3. Exemptions from credentialed scans only will granted for legitimate business reasons
4.4. Applicable reports from network scans will be made available to the corresponding IT unit based on procedures defined by IT staff performing network scans.
4.5. IT units are responsible for using network scan reports to validate their patching processes and compliance based on standards and procedures approved by the IT Security Council and KMIT Ops.

5. Exceptions

5.1. Exceptions must be documented and reported to the HSC ISO (Information Security Officer) through the Unit Security Liaison as required in Policy *HSC-200 Security and Management of HSC IT Resources*.

Item	Contact	Date	Approval
Owner	Barney Metzner, HSC ISO, HIPAA Security Officer		
Committee(s)	HSC IT Security Council HSC KMIT OPS Committee		Y

Official Approver	Holly Buchanan, HSC CIO Glen Jornigan, UNMH IT Administrator Barney D. Metzner, HSC ISO, HIPAA Security Officer	Y
Official Signature(s)		

Effective Date:	
Origination Date:	
Issue Date:	

DOCUMENT APPROVAL & TRACKING

DRAFT