Subject: **Information Security**	Page **1 of 5**	Policy # **Version: 1.1**
Title: **Patch Management**	Revision of: **Version 1.0, 12/31/2017**	Effective Date: **4/9/18**
		Removal Date:

I. PURPOSE

This policy establishes the patch management program and oversight for the Northwestern University (NU) Feinberg School of Medicine (FSM). Patch management will implement patches and system updates that are required to manage security risks posed by internal and external threats.

The scope of this policy includes servers, endpoints, printers, IoT devices (e.g., freezer monitors, IP cameras) and other software components that enable applications (e.g., database, middleware/connector software, plug-in, development platforms) whether hosted at NU, FSM or externally (e.g., third-party, cloud services) or FSM IT centrally managed or managed by a FSM Department/Center/Institute.

This augments the guidance provided from the Northwestern Information Technology (NIT) Management of Patch and System Update Guidelines and is a complement to the FSM Vulnerability Management Policy.

II. PERSONS AFFECTED

NU FSM IT staff, NU FSM System / Application Administrators and NU FSM and FSM Department/Center/Institute application developers and support.

III. POLICY STATEMENT

Patches and software updates will be applied within the Patch Cycle and Remediation schedule defined in the Procedure.

When possible, test environments will be leveraged to ensure the impact of changes are identified and evaluated prior to production implementation.

Emerging threats such as zero-day exploits and ransomware will require urgent evaluation and implementation of patches, software updates, forced reboots, port blocking and/or configuration changes within a timeframe as agreed by FSM IT leadership and as defined for Emergencies in the Procedure.

FSM IT will coordinate directly with system / application owners of business critical services for scheduling implementation of patching and software updates as required by the Procedure and to ensure adequate contingencies and recovery procedures in case of failure or error.

Patch management will be an ongoing process and must follow appropriate and approved procedures, which includes defining baselines and developing plans for risk categorization, evaluation, documentation, communication, testing, back out capability and implementation.

Remediation activities including proper documentation of the change, testing, sign-offs from system / application owners, and back out plans must be reviewed and coordinated through FSM IT Change Management Process.

Any exceptions, including exemptions of systems or applications from patching and updates (e.g., laboratory systems, vendor turnkey systems, integrated or standalone systems using unsupported operating systems, IoT systems) must be documented in writing with mitigation steps and approved by the FSM IT Steering Committee through the Procedures defined in the FSM Security Risk Management Policy.

IV. PROCEDURE STATEMENT

Identification / Classification

FSM IT will maintain an ongoing inventory of servers, endpoints, and standard applications with appropriate documentation (e.g., IP addresses, business / technical contacts, etc.) to facilitate prioritization and implementation of patches.

FSM IT will maintain patch baselines with minimum requirements based on operating system level, service pack, hotfix, and patch level.

Asset Risk Classification

Asset risk classification is defined in the Vulnerability Management Policy.

Patch Cycle and Remediation

Remediation will be prioritized based on the asset risk classification and the patch severity level.

		Asset Risk Classification		
FSM Risk Level	**Qualys Score**	**High**	**Medium**	**Low**
Emergency*	N/A	< 48 hours	< 3 days	< 7 days
High	4-5	< 30 days	< 30 days	< 30 days
Medium	2-3	< 60 days	< 60 days	< 60 days
Low	1	< 90 days	< 90 days	< 90 days

*FSM IT leadership may determine that implementation of patches and updates to mitigate emergencies may require shorter response times, on a case by case basis. Forced reboots, immediate configuration changes, and port blocking may be necessary contain risks to high risk assets.

Roles and Responsibilities

The scope of this policy includes servers, endpoints, printers, IoT devices (e.g., freezer monitors, IP cameras) and other software components that enable applications (e.g., database, middleware/connector software, plug-in, development platforms) whether hosted at NU, FSM or externally (e.g., third-party, cloud services) or FSM IT centrally managed or managed by a FSM Department/Center/Institute.

FSM IT Client Management will oversee the implementation of patching and software updates on FSM endpoints and standard image-based applications (e.g., Microsoft Office, plug-ins) on Tier 1 and Tier 2 networks.

FSM IT Infrastructure will oversee the implementation of patching and software updates of servers and applications in the NU-hosted datacenter environment.

FSM IT Security will oversee the patching policy and provide oversight, direction and reporting regarding compliance.

FSM IT Application Development will develop a plan for the implementation, prioritization and upgrade scheduling of patching and security updates that are identified as a risk to managed applications

FSM Department/Center/Institute Application Development will develop a plan for the implementation, prioritization and upgrade scheduling of patching and security updates that are identified as a risk to department applications.

FSM Change Advisory Board will be responsible for approving requested changes and assisting in the assessment and prioritization of the routine and emergency patch management deployment requests.

FSM IT Steering will agree upon risk ratings, prioritization, remediation options and exceptions to this Policy.

Monitoring and Reporting

Metrics must be compiled and maintained summarizing the outcome of each patching cycle and must be made available to the responsible parties in the Roles and Responsibilities section.

Reports must be routinely reviewed to assess the benefit or risk associated with implementation, and determine a course of action.

Remediation will be tracked through support tickets and reviewed by the FSM Change Advisory Board (CAB).

V. REVISION HISTORY

12/31/17 – New policy effective.
4/9/18 – Aligned patch cycles with Vulnerability Management Policy.

VI. DEFINITIONS

Middleware: Software that serves to "glue together" separate, often complex and already existing, programs. Some software components that are frequently connected with middleware include enterprise applications and Web services. Middleware often sits between the operating system and applications on different servers and simplifies the development of applications that leverage services from other applications.
http://searchmicroservices.techtarget.com/definition/middleware

Connector: Software that governs interactions/communication between components of an overall application architecture.
http://www.ics.uci.edu/~taylor/classes/221/07_Software_Connectors.pdf

Plug-in: Software component that adds a specific feature to an existing program (e.g. web browser Adobe Flash, Java)

VII. RELEVANT POLICY REFERENCES

FSM Security Risk Management Policy
http://www.feinberg.northwestern.edu/it/docs/feinberg_it_security_risk_management_policy_11_01_17.pdf

FSM Vulnerability Management Policy (approved, to be published)

Management of Patch and System Update Guidelines
Northwestern Information Technology (NIT) Management of Patch and System Update Guidelines

VIII. TECHNICAL REFERENCES

National Vulnerability Database (NIST)
https://nvd.nist.gov/

Common Vulnerabilities and Exposures (US-CERT)
https://cve.mitre.org/

Common Vulnerability Scoring System v3.0: Specification Document
Section 2.3 Impact Metrics (High, Medium, Low defined)
https://www.first.org/cvss/specification-document

Qualys
https://www.qualys.com/research/security-alerts/

Microsoft (Critical, Important, Moderate, Low defined)
https://technet.microsoft.com/en-us/security/gg309177.aspx

Red Hat
https://access.redhat.com/security/updates/classification

Cisco
https://tools.cisco.com/security/center/home.x

Apple
https://support.apple.com/en-us/HT201222

BigFix – Identifying Security Patches
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/Identifying%20Security%20Patches

NIST Special Publication 800-40 Rev. 3 Guide to Enterprise Patch Management Technologies
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Surviving Insecure IT: Effective Patch Management
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901613