Subject: **Information Security**	Page **1 of 6**	Policy # **Version: 1.1**
Title: **Vulnerability Management Policy**	Revision of: **Version 1.0, 12/31/17**	Effective Date: **4/9/18**
		Removal Date:

I. PURPOSE

This policy and procedure establishes the framework for the Northwestern University (NU) Feinberg School of Medicine (FSM) vulnerability management program. Vulnerability management will identify technical risks to on premise and off premise (e.g., service providers, cloud services) servers, endpoints, and applications that comprise the FSM technology environment. Through risk-based remediation, the risk of unauthorized disclosure of sensitive information can be reduced. This augments the guidance provided from the Northwestern Information Technology (NIT) Assessment Program.

II. PERSONS AFFECTED:

All NU and FSM IT leadership, NU FSM Dean's Office Administration, NU FSM IT staff, and all NU FSM System / Application Administrators.

III. POLICY STATEMENT

The scope of this policy includes on premise and off premise (e.g., service providers, cloud services) servers, endpoints, and applications within the FSM IT managed environment and applications which are managed within FSM Departments/Centers/Institutes. Where FSM uses University shared resources, FSM will coordinate vulnerability management with NIT.

Vulnerability management will be applied on a risk basis with the highest priority where ePHI and personally identifiable information resides.

In some cases, immediate response and remediation will be necessary to mitigate risk of zero-day threats and other threats of imminent danger to FSM or the University.

Vulnerability management will be a continuous process consisting a routine and periodic testing using a variety of techniques and information resources for vulnerability assessment, penetration assessment and penetration testing; a remediation process; and ongoing executive reporting to FSM IT Steering as defined by the Procedure.

The FSM IT Security team will manage the Vulnerability Management process which will include conducting tests and reporting upon risks to the operational support teams within FSM IT. FSM will leverage the tools for vulnerability assessments and penetration assessments as provided by NIT.

Reporting of risks will be categorized as defined in the FSM Risk Management policy.

Remediation activities will be implemented according to the FSM Patch Management Policy which includes coordination through FSM IT Change Management Process. Configuration changes will be implemented through the FSM IT Change Management Process. In cases where a vulnerable application is not managed by FSM IT, the System / Application Administrator is required to remediate vulnerabilities in accordance with remediation timelines as outlined in the FSM Patch Management Policy.

Any exceptions, including exemptions of systems or applications from the vulnerability management program, must be documented in writing and approved by the FSM IT Steering Committee.

IV. PROCEDURE STATEMENT

Identification / Classification

FSM IT will maintain an ongoing and updated inventory of assets and applications. The inventory will include all assets and related scan targets (IP addresses, IP ranges, etc.) as well as authorized software and applications.

FSM IT Security will conduct monthly scans on all subnets for the purpose of identifying new devices. Any rogue devices or servers identified to be running on endpoint subnets will be immediately investigated and reported to FSM IT operational support teams.

Servers, business critical applications, and endpoints will be given an asset risk classification for purposes of prioritizing scans.

Asset Risk Classification

The highest level of data sensitivity on an asset defines the level of the asset risk. Data sensitivity is defined in the NU Data Access Policy.

	Servers, Business Critical Applications or Services	**Endpoints**
Asset Risk	**Data Sensitivity**	
High	-Presence of ePHI or PII -Internet facing FSM business critical applications	-Presence of ePHI or PII on Tier 2 endpoints -Tier 1 endpoints
Medium	-Data used in research which is not individually identifiable	-Data used in research which is not individually identifiable on Tier 2 endpoints
Low	-No risk or consequence if data accessible or exposed publically	-No risk or consequence if data accessible or exposed publically -Tier 3 endpoints

Vulnerability Scans

Vulnerability scans will be conducted according to the following frequency:

Risk	**Vulnerability Scan Frequency***
High	30 days
Medium	60 days
Low	90 days

Additional considerations and restrictions:

- FSM IT Security will recommend to the Northwestern Memorial Hospital (NMH) security team scheduling and frequency regarding the execution of vulnerability scans on Tier 1 endpoints. Scanning of Tier 1 endpoints will be conducted by NMH.
- Scans of cloud services will be scoped to and will comply with cloud service provider policies (including AWS and Azure penetration testing policies).
- The potential impact of scans on the availability of an asset will be assessed prior to conducting a scan.

Penetration Assessments

Penetration assessments will be conducted on application systems which use confirmed ePHI or business critical administrative PII. FSM will leverage the tools for vulnerability assessments and penetration assessments as provided by NIT.

Penetration assessments will be conducted prior to the launch of new or significantly revised application systems and for existing systems on an annual basis.

Penetration Testing

Penetration testing will be conducted on application systems which use confirmed ePHI or business critical administrative PII. Determining the need for penetration testing will consider the results of penetration assessments. Coordination and execution of penetration testing will be coordinated with the FSM IT Steering Committee and NIT. External security services expert at performing penetration testing will be engaged to do this work.

Frequency and scope of penetration testing will be on an as needed basis.

Remediation

FSM IT Security will review and prioritize vulnerabilities into risk categories. Remediation (e.g. patching, configuration changes, software removal) will be prioritized according to asset risk classification and categorization of risks as defined in the FSM Risk Management policy.

Appendix A maps the severity level provided the current NIT vulnerability scanning tool to risk levels defined by the FSM Risk Management Policy.

Vulnerabilities listed as "potentially existing" will be assessed on a case by case basis. FSM IT Security will conduct further investigation and testing against the device or application to determine with more certainty whether the vulnerability actually exists. If determined to be likely to not exist, the potential vulnerability will be downgraded in severity class by one level, but will still be included in list of vulnerabilities to remediate.

Remediation Timelines (i.e., SLAs) are defined in the Patch Management Policy.

Remediation timelines may be escalated at the discretion of FSM IT leadership.

Resolution will be accomplished via patching, software updates, configuration changes and/or procedure changes.

If remediation isn't undertaken within the timeframes defined by the SLAs, reporting will occur to FSM IT leadership, the SLA breach will be recorded in the FSM Risk Registry as defined in the FSM Risk Management Policy and disposition of further actions (e.g., shut down of the device or application) determined by the FSM IT Steering Committee.

Reporting

The FSM IT security team will report all vulnerabilities to the appropriate System / Application Administrator, along with the required timeline to remediate the vulnerability. For FSM IT managed systems or applications, remediation will be tracked through support tickets and reviewed by the FSM Change Advisory Board (CAB). For FSM department managed applications, remediation progress will be reported to the FSM IT Steering Committee.

FSM IT Security will maintain metrics for monthly reporting to NU and FSM IT leadership. Metrics will include:

- Remediation SLA compliance rate
- SLA breaches
- List of vulnerabilities in breach of remediation SLA
- Average vulnerability risk by device category
- Number of existing critical vulnerabilities

Exceptions to the SLAs may be recorded in the Risk Registry as defined in the FSM Risk Management policy.

V. DEFINITIONS:

System / Application Administrator: The individual or group that is responsible for configuration and maintenance of a system or application.

Legally/Contractually Restricted Data: Data that is required to be protected by applicable law or statute (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act), or which, if disclosed to the public could expose the University to legal or financial obligations. See NU Data Access Policy.

VI. POLICY UPDATE SCHEDULE:

Policy review to occur one year after initial implementation and every three years thereafter.

VII. REVISION HISTORY:

12/15/17 – New policy effective.
4/9/18 – Aligned scan and remediation schedules with Patch Management Policy.

VIII. RELEVANT REFERENCES:

FSM Risk Management Policy:
http://www.feinberg.northwestern.edu/it/docs/Feinberg-IT-Security-Risk-Management-Policy-11_01_17.pdf

NIT Vulnerability Assessment Program:
http://www.it.northwestern.edu/security/vulnerability-assessment/index.html

NU Data Access Policy:
http://www.it.northwestern.edu/policies/dataaccess.html

NIST SP 800-40 Ver. 2: Creating a Patch and Vulnerability Management Program:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-40ver2.pdf