ADMINISTRATIVE POLICY

Subject: **Information Security**	Page: **1 of 5**	Policy # Version: **1.1**
Title: **FSM Web Application Maintainability**	Revision of: **1.0**	Effective Date: **8/15/2025**
		Removal Date:

I. PURPOSE

The purpose of this policy is to promote the secure, sustainable, and compliant development of web applications that support the research, educational, and administrative activities of the Northwestern University (NU) Feinberg School of Medicine (FSM). As web applications often interact with sensitive data and institutional systems, this policy helps ensure risks are appropriately managed through defined standards for ownership, security, and lifecycle maintenance.

II. POLICY STATEMENT

All web applications used for official FSM business purposes, whether developed internally, contracted through a vendor, or commercially purchased, must have a defined plan for ongoing support, maintenance, and compliance.

This maintenance must:

- Be hosted on FSM-approved platforms or cloud services.
- Be registered and reviewed by FSM IT prior to deployment.
- Include clearly defined business and technical ownership.
- Comply with all applicable FSM and NU policies, technical standards, and relevant legal or regulatory data protection requirements.
- Include a documented support plan that outlines the application's lifecycle, including patching, maintenance, and decommissioning.

Web applications are also subject to branding and logo usage requirements defined in the FSM Website Development and Governance Policy.

III. PERSONS AFFECTED

All FSM faculty (including adjunct, emeritus, and visiting), staff, students, residents, fellows, contractors, vendors, and any individuals with access to FSM data, systems, or facilities.

IV. DEFINITIONS

Web Application – An interactive tool or system that requires user authentication, input, or complex data handling.

Website – A static or semi-static collection of public web pages intended to communicate information about FSM-related activities.

V. PROCEDURE STATEMENT

To ensure accountability, security, and ongoing operational support, each software application must have both a designated Business Owner and Technical Owner:

Business Owner

- Must be a full-time faculty or staff member, typically the Principal Investigator (PI) or senior departmental administrator.
- Responsible for justifying the application's purpose, ensuring alignment with institutional priorities and compliance expectations, and overseeing lifecycle decisions.

Technical Owner

- May be an FSM faculty/staff member, student, approved contractor, or vendor with a formal agreement with NU.
- If the Technical Owner is a vendor, an FSM-affiliated technical contact must be designated who understands the core functionality and can coordinate with FSM IT as needed.

Governance

- Applications must comply with the FSM Website Development and Governance Policy, including requirements related to branding, naming conventions, and custom domain use.
- Security and operational terms must be addressed through a formal contract when third-party involvement exists, including vendor-developed or commercially procured applications.
- All such contracts must comply with the NUIT Security Addendum to ensure appropriate security controls are followed.

- Web applications must use NU's NetID authentication whenever feasible. If public account creation is necessary, applications must implement secure authentication practices, including strong passwords, secure credential storage, and session protections. Default, shared, or hard-coded credentials are prohibited. All authentication methods for publicly accessible applications must be reviewed and approved by FSM IT.

Platforms & Standards

- FSM IT must be consulted and provide approval during technology selection to ensure platforms are modern, secure, supported, and meet institutional accessibility standards.
- Applications must follow current industry best practices and avoid unsupported development methods.
- Where possible, existing FSM-approved applications should be reused to minimize redundancy.
- Third-party developed applications must maintain a separation of development and production environments.
- Before deployment to production, all web applications must undergo vulnerability scanning, with identified issues remediated or formally mitigated in coordination with FSM IT.
- FSM- and NU- supported tools and deployment workflows should be used when applicable.
- Platforms must align with the application's codebase and technical needs.

Content & Ownership

- A full-time FSM faculty or staff member must be assigned to oversee the application's continued justification and compliance.
- All application content must adhere to the NU Digital Accessibility Policy.
- Application ownership must be defined in collaboration with NU's Innovation and New Ventures Office (INVO), where applicable.

Lifecycle & Data Retention

- Each application must have a lifecycle plan that addresses patching, support, and decommissioning.
- Orphaned or outdated applications will be archived or removed by FSM IT.
- Once a study or project ends, applications must be taken down and archived per NU policy or sponsor contract.

- Data must be retained in accordance with the NU Research Data Retention Policy or any applicable sponsor, legal, or regulatory obligations.
- If the application is tied to a study or grant, an expected hosting end date must be provided at the outset.

VI. EXCEPTIONS

Exceptions to this policy require approval by the FSM Dean's Office. Exceptions may be revoked if used inappropriately or if they introduce risk to the institution. Please submit exception requests to fsmit-policy@northwestern.edu.

VII. COMPLIANCE AND ENFORCEMENT

Compliance with this policy may be reviewed as part of periodic IT security assessments. Web applications found to be non-compliant must submit a remediation plan to fsmit-policy@northwestern.edu within 30 days. For legacy systems where full compliance is not feasible, FSM IT will implement mitigation steps to reduce security and operational risks.

VIII. POLICY UPDATE SCHEDULE

This policy will be reviewed annually and updated as necessary to remain aligned with NU policies, standards, regulatory requirements, and evolving technology practices.

IX. RELEVANT REFERENCES

FSM Website Development & Governance Policy
https://www.feinberg.northwestern.edu/policies/documents/website-development-policy.pdf

NU Research Data: Ownership, Retention, and Access
https://researchintegrity.northwestern.edu/resources/research-data-policy.pdf

NU Endpoint Security Standard
https://www.it.northwestern.edu/about/policies/endpoint-security.html

NU Patch Management Standard
https://www.it.northwestern.edu/about/policies/patchmanagement.html

NU Digital Accessibility Policy
https://policies.northwestern.edu/docs/digital-accessibility-policy-final.pdf

X. CONTACT INFORMATION

For general IT support or to report an incident, please contact fsmhelp@northwestern.edu.

For questions, clarifications, or requests for exceptions related to this policy, please contact fsmit-policy@northwestern.edu.