

ADMINISTRATIVE POLICY

Subject: Information Security	Page 1 of 3	Policy # Version: 1.0
Title: Data Backup Policy	Revision of: New policy	Effective Date: 2/28/18
		Removal Date:

I. PURPOSE

This policy and procedure establishes the required actions to ensure administrative data and research data including electronic Protected Health Information (ePHI) and personally identifiable information (PII) used by the Feinberg School of Medicine (FSM) is backed up, safely stored and is accessible and available to restore ongoing operations with minimal disruption.

Regular data backups reduce the risk of permanent data loss which can occur for many reasons including computer theft, hardware failure, power loss and security compromises.

II. PERSONS AFFECTED:

All NU FSM faculty, staff and students.

III. POLICY STATEMENT

FSM research and administrative data (e.g., ePHI, PII) is required to be backed up with a copy stored offsite. Copies of data stored offsite copies must be encrypted.

It is the responsibility of Principal Investigators and FSM business leaders (e.g., Department Administrators, Deans Office) in collaboration with NU and FSM IT to ensure a data backup and offsite storage plan has been implemented. These plans must meet the data restoration time frames required to support FSM research projects and administrative operations.

For NU IRB approved FSM research projects a backup plan is required to be documented as part of the [Data Security Plan](#).

Periodic testing of data backup/restoration procedures are required to ensure backup copies are usable.

The use of personally owned computing devices or portable data storage media, unapproved NU or FSM services or home/apartment locations, vehicles and smart-phone devices are not permitted for data backup and offsite storage plans.

IV. PROCEDURE STATEMENT

Data stored on NU file servers including individual and shared mapped drives from endpoint devices (e.g., FSMRESFILES), Sharepoint, NU Box, Research Data Storage and email services automatically include backup and offsite services.

Title: Data Backup Policy	Page 2 of 3	Policy # Version: 1.0
-------------------------------------	-----------------------	---------------------------------

Files, databases and applications which reside on FSM servers will need to have a backup and offsite storage plan.

Data stored on FSM IT managed endpoint devices (e.g. desktop, laptop computers) will need to have CrashPlan Pro installed and configured using [NU Central Desktop/Laptop Data Backup Service](#).

Data stored in laboratory systems and standalone or turnkey systems not covered by the above procedures will need to have a backup and offsite storage plan.

The use of external vendors or research partners for data storage including those provided through external vendors or a Cloud service providers are permitted provided there is a data backup and offsite storage plan verifiable under an approved NU or FSM contract. In the absence of a verifiable plan, a custom backup and offsite storage plan may need to be developed.

For assistance with confirming and establishing a backup plan please send your inquiry to FSMHELP@northwestern.edu.

For questions about Data Security Plans please send your inquiry to FSMIT-policy@northwestern.edu.

Any exceptions to this Policy and Procedure must be documented in writing and approved by the FSM IT Steering Committee.

V. POLICY UPDATE SCHEDULE:

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

VI. REVISION HISTORY:

2/28/18 – New policy effective.

VII. RELEVANT REFERENCES:

NU Central Desktop/Laptop Backup Service
<http://www.it.northwestern.edu/dss/backup-service/>

Data Security Plans for Information Used in Clinical Research
<http://www.feinberg.northwestern.edu/it/policies/information-security/data-security-plans.html>

File Sharing at Northwestern
<http://www.it.northwestern.edu/file-sharing/overview.html>

FSM File Storage
<http://www.feinberg.northwestern.edu/it/services/storage-options.html>

NU Business Continuity Planning Policies
<http://www.northwestern.edu/bcp/>

Title: Data Backup Policy	Page 3 of 3	Policy # Version: 1.0
-------------------------------------	-----------------------	---------------------------------

Rights and Responsibilities for the Use of Central Network and Computing Resources at Northwestern University:

<http://www.it.northwestern.edu/policies/responsibilities.html>

FSM Security Risk Management Policy:

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