ADMINISTRATIVE POLICY

Subject: **Mobility**	Page **1**	Policy # Version: 1.0
Title: **Device Security Policy**	Revision of: **New Policy**	Effective Date: **04/15/2016**
		Removal Date:

I. PURPOSE

Connectivity through the rapid evolution of mobility continues to drive significant improvements in data sharing, decision making and overall productivity across a diversity of devices. This includes Feinberg School of Medicine Central IT (FSM IT) managed, mobile, and personal devices. While Northwestern University's (NU) Feinberg School of Medicine embraces these important advancements, it does introduce increased risk of data loss and theft due to differing methods of data storage and data protection. Additional safeguards in this Policy are intended to reduce these data risks and the potential negative effect it may have on our research participants, programs and employees as well as to NU's regulatory and financial posture.

II. POLICY STATEMENT

All devices that are FSM IT managed, FSM department managed or personally-owned and access any type of non-public NU data are in scope to this Policy. This includes devices which are connected directly to the NU network and/or remotely connected to the NU network through NU SSL VPN remote access.

Devices are further defined as follows:

- FSM IT managed devices are configured, deployed, and managed by central FSM IT (e.g., desktops, laptops and tablets) per approved standards.

- FSM department managed devices are configured, deployed, and managed by an FSM department following central FSM IT approved standards.

- Mobile devices are laptops, tablets, smartphones or any of their functional equivalent.

- Smartphone devices are any device running Apple iOS, WatchOS, Windows Phone or Android OS with enabled carrier (e.g., AT&T, Verizon) connectivity or any of their functional equivalent.

- Personal devices include mobile devices, home-based, personally-owned equipment, and smartphone devices.

III. PROCEDURE STATEMENT

The following are required of **all devices** accessing non-public NU systems and data. Refer to additional procedures for **smartphone device** usage below.

a. No non-public NU data (e.g., research, healthcare/clinical, student data) will be permitted to be stored on mobile and personal devices, unless they are FSM IT managed devices. This includes, but is not limited to, attachments saved from email messages, forwarded email from

NU email systems to commercial email systems, and any NU data copied from NU secure storage. See the allowances for smartphones below.

a. The device must be encrypted.

b. All lost, stolen or compromised devices must be immediately reported to fsmhelp@northwestern.edu.

c. The following device characteristics are required and must be configured as follows:
- Device pin (six position) or complex password as defined by NU policy
- Device lockout after 10 invalid pin or password entries
- Idle timeout (at maximum of 15 minutes)
- Agree to and enable remote wipe due to loss or theft of device
- OS, applications and anti-malware (if applicable) maintained to current patch levels
- No jailbroken or rooted devices are allowed
- Security features of device are never to be disabled

d. Compliance with these safeguards may be verified prior to allowing a connection to the NU network.

e. All data must be wiped prior to decommissioning, disposal and transfer of ownership.

f. Access to non-public NU data is permitted only through NU SSL VPN remote access http://www.it.northwestern.edu/oncampus/vpn/sslvpn/

The following are required of all **smartphone devices** accessing non-public NU systems and data:

a. All mobile devices are required to be encrypted and to use a PIN with a minimum length of six. Please note that using a PIN does not necessarily mean the device is encrypted. For Android devices encryption must be enabled in addition to establishing a PIN. NU mobile device security guidelines are located here: http://www.it.northwestern.edu/policies/mobile-devices.html

b. NU procedures to establish a PIN for the purposes of accessing NU email on your smartphone are located here: http://www.it.northwestern.edu/collaborate/how-to/mobile.html

c. No more than 30 days of NU email is allowed to be retained on the smartphone device. See instructions below, Limiting Days to Sync Email.

FSM IT Customer Support services can implement encryption and PIN setting of FSM IT managed devices including smartphones and to also provide encryption guidance for other mobile and personal devices. Please contact fsmhelp@northwestern.edu.

IV. PERSONS AFFECTED

All NU Feinberg School of Medicine faculty, staff, students, residents, and fellows accessing or storing any type of non-public NU data using FSM IT-managed devices and/or personally-owned mobile and/ or personal devices.

V. POLICY UPDATE SCHEDULE

No less than every five (5) years, but more frequent updates may be conducted as required.

VI. DEFINITIONS

FSM IT Managed Devices – Devices such as desktops, laptops, and tablets configured, deployed and managed by central FSM IT per approved standards.

FSM Department Managed Devices - Devices configured, deployed and managed by an FSM department following FSM IT approved standards.

Mobile Devices – Laptops, smartphones, tablets or any of their functional equivalent.

Personal Devices – Any device not directly supported, configured and managed by FSM IT and will encompass but is not limited to mobile devices and home-based, personally-owned equipment.

Smartphone Devices - Any device running Apple iOS, WatchOS, Windows Phone, or Android OS with enabled carrier (e.g., AT&T, Verizon) connectivity or any of their functional equivalent.

Complex Password* – Composition consistent with NU NetID password/passphrase requirements (i.e., 8-31 characters in length and contain a non-alphanumeric character).

Non-public NU Data – Non-public data is information that is not published with public accessibility (e.g., phone directory via an Internet web-site).

VII. REVISION HISTORY

04/15/2016 - New policy effective.

VIII. RELEVANT REFERENCES

Collaboration Services – Mobile Support Tools
http://www.it.northwestern.edu/collaborate/how-to/mobile.html

Feinberg Information Technology Standards & Policies:
http://www.feinberg.northwestern.edu/it/standards-policies/index.html

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

Feinberg Information Technology – Storage Options
http://www.feinberg.northwestern.edu/it/services/storage-options.html

Mobile Device Security Guidelines (NUIT)
http://www.it.northwestern.edu/policies/mobile-devices.html

NetID Password/Passphrase*
http://www.it.northwestern.edu/netid/password.html

Disposal of Northwestern University Computers
http://www.it.northwestern.edu/policies/disposal.html

Management of Patch and System Update Guidelines
http://www.it.northwestern.edu/policies/patches.html

SSL VPN Overview
http://www.it.northwestern.edu/oncampus/vpn/sslvpn/

Disposal of Northwestern University Computers
http://www.it.northwestern.edu/policies/disposal.html

IX. LIMITING DAYS TO SYNC EMAIL

a. iPhone (iOS 9.2.1)

Select or enter the following steps:

Settings
Mail, Contacts, Calendars
Accounts (NU Outlook)
Mail Days to Sync
Select “1 month” option

b. Android (5.1.1)

Select or enter the following steps:

Email
More (at upper right)
Settings
Accounts (NU email address)
Period to sync email (select “1 month”)