University System
of New Hampshire

SECURITY STANDARDS FOR MOBILE DEVICES

Responsible Executive/University Officer: Chief Information Security Officer
Responsible Office: ET&S Cybersecurity GRC
Approved Distribution: Public
Status: IN EFFECT

1. Purpose

The purpose of this standard is to provide acceptable use and security guidance to USNH employees for protecting USNH data stored on or accessed through personally owned or institutionally provided mobile devices such as smartphones (e.g., iPhones, Android phones, Windows phones etc.), tablet computers such as iPads, and other Personal Digital Assistants (PDAs).

Examples of situations in which this standard may apply includes:

- Syncing a mobile device to university provided email (through Microsoft active sync, etc.).
- Downloading non-public university documents to the mobile device.

This standard does not apply if the mobile device is just used to browse public information available without any authentication on USNH's websites.

2. Scope

This Standard applies to all USNH staff, faculty, students, and affiliates.

3. Standard

3.1 Do not store Restricted or Protected USNH data (including sensitive student data, Protected Health Information and Social Security Numbers, etc.) on personal mobile devices. Mobile device users who do have a valid business need to store non-public data must seek guidance regarding additional controls from appropriate Data Stewards or ET&S Cybersecurity. Additional protection may include encryption of data, passwords, automatic logoffs, and secure Internet transmissions.

3.1.1 USNH employees are expected to secure devices to prevent unauthorized access whenever they are left unattended.

3.1.2 USNH employees should provide a notification to the campus Help Desk as soon as possible in the event of a lost or stolen device containing university data.

3.1.3 Mobile devices are recommended to have at least a 4-digit PIN to authenticate and an inactivity timeout of 15 minutes.

3.2 Whenever possible, USNH mobile devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.

3.3 All persistent storage within mobile devices will be encrypted.

3.4 Disposal of University Mobile Devices are required to follow the SEED Process.

3.5 Data stored on mobile devices should be properly purged of all USNH information before the device is disposed, donated, or an employee's relationship with the University is terminated.

4. Exceptions

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the Cybersecurity Exception Standard

5. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to institutional resources or termination of employment. Students may be referred to Student Affairs for discipline. A violation of this policy by a temporary worker, contractor, or vendor may result in action up to and including termination of their contract or assignment with USNH.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

DOCUMENT HISTORY

Effective Date:	May 27, 2022
Approved by:	Thomas Nudd, Chief Information Security Officer, August 24, 2022
Reviewed by:	Dr. David Yasenchock, Directory Cybersecurity GRC, August 24, 2022
Revision History:	USNH Cybersecurity GRC Standards Committee, August 24, 2022 Revised formatting, K SWEENEY, February 1, 2024