University System of New Hampshire

SECURITY STANDARDS FOR MOBILE DEVICES

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

1. Introduction

The purpose of this standard is to provide related 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 these standards may apply include:

- Syncing the mobile devices 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. Standards

- 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, the use of passwords, automatic logoffs, and secure Internet transmissions.
- USNH employees are expected to secure devices to prevent unauthorized access whenever they are left unattended.
- USNH employees should provide a notification to the campus IT Help Desk as soon as possible in the event of a lost or stolen device containing university data.
- Mobile devices are recommended to have at a minimum a 4-digit PIN to Authenticate and an inactivity timeout of not more than 15 minutes.
- Whenever possible, USNH mobile devices will include the ability to remotely wipe stored data in the event the device is lost or stolen.
- All persistent storage within mobile devices will be encrypted.

Disposal

University System of New Hampshire

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

3. CONTACT INFORMATION

For USNH community members: Questions about this standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, & Compliance (GRC) via this Support Form.

A community member may submit other requests here: Submit an IT Question.

---

4. DOCUMENT HISTORY

Effective Date: May 27, 2022
Drafted: Dave Yasenchock. August 24, 2022 v02
Revised, USNH Cybersecurity GRC Standards Committee, August 24, 2022
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, August 24, 2022
Approved by: Thomas Nudd, Chief Information Security Officer, August 24, 2022