Section 1: Introduction

This document defines Bucknell University’s policy for the secure use of mobile and remote devices which access any information resources owned or managed by the University.

Mobile and remote devices are important tools for the University, and their use is supported to advance our academic mission. However, mobile and remote devices also represent a significant risk to information security and data security. If appropriate security applications and procedures are not applied, mobile and remote devices can serve as a conduit for unauthorized access to the institution’s data and IT infrastructure that can subsequently lead to data leakage and system infection.

Bucknell University faculty, staff, students, student employees, and volunteers who use mobile or remote devices are responsible for all institution data, which is stored, processed and/or transmitted via that device, and for following the security requirements set forth in this policy. Any device that does not meet the requirements specified in this policy may not be used to access or store any University data that is classified as Sensitive or Confidential.

Whenever practical, elements of this policy will be enforced via centrally administered technological controls. Bucknell University may request proof of compliance from any user of a Mobile or Remote device for any policy issues that cannot be automatically managed or enforced.

Section 2: Definitions

2.1: Users

User: Any faculty, staff, student, student employee, volunteer or agent of the above who uses a mobile or remote device to access any non-public information systems owned or managed by the University.

2.2: Data Classifications

Sensitive data is institutional information that must be guarded due to proprietary, ethical, privacy, or business process considerations. Sensitive data must be protected from unauthorized access, modification, transmission, storage or release.

Confidential data is institutional information protected by government regulations, statutes, industry regulations, contractual obligations, or specific University policies. Administrators and data stewards may designate additional types of institutional data as confidential.

For more information about data classifications, see the Data Classification Policy at <WEB-LINK>.

2.3: Devices & Media

Mobile Device: Any electronic device that is easily transported, communicates via wireless technology (cellular services, Wi-Fi, etc.), and is used to access University information systems or store sensitive or confidential information. Examples include: laptops, smartphones, and tablets.
Remote Device: Any self-contained computing or storage device not physically tethered at the Bucknell University campus that is used to access or store sensitive or confidential information. Examples include: personal home computers, University-owned laptops, CD/DVD media discs, portable hard drives, and flash drives.

For the purposes of this policy, devices are not restricted to those owned by the University. Furthermore, a device can be both mobile and remote – i.e., a University-owned laptop that is used on campus and from home.

Section 3: Required Device Configurations and Capabilities

3.1: Configurations for Mobile Devices

All users of a mobile electronic device must take the following measures:

- Configure the device to require a password, biometric identifier, PIN, or swipe gesture to be entered before local access to the device is granted.
- Enable a screen lock or similar mechanism to require the password, PIN, or swipe gesture to be entered after an idle time of at most five minutes.
- Enable the device’s automatic wipe functionally to occur after a sequence of no more than ten unsuccessful attempts to unlock the device.
- Register the device with a remote wipe service to permit a lost or stolen device to be securely erased.

3.2: Configurations for Remote Devices

Users of personally owned remote devices must take the following steps:

- Configure the operating system to automatically download and install system patches and updates.
- Ensure that an Library and IT (LIT) approved anti-virus package is installed, operational, and configured to automatically download and install signature updates.

3.3: Encryption of Data in Transit

Sensitive and Confidential information must be encrypted while in transit from the Bucknell network to any device. Transit encryption services will be provided by the institution or the appropriate software vendor, and/or by the use of a secure Virtual Private Network (VPN) connection.

3.4: Encryption of Data at Rest

Except when being actively viewed on a device, Confidential information must at all times be encrypted on that device through a mechanism approved by the institution.

Approved encryption mechanisms include:

- Microsoft BitLocker (Windows)
- File Vault (Apple OSX)
- TrueCrypt (multi-platform)
Section 4: User Responsibilities

4.1: Required Actions for Lost or Stolen Devices

Upon determining that devices have been lost or stolen, device owners must as soon as possible:

1. Report the loss or theft to the LIT Techdesk and other offices as appropriate.
2. In conjunction with the LIT Techdesk, invoke the remote wipe functionality to securely erase the contents of the device.
3. Reset his or her University password(s).

4.2: Required Actions for Decommissioned Devices

In the event that a mobile device is to be sold, traded, or recycled, the primary user must securely erase the contents of the device while it is still in his or her possession.

4.3: Backups and Encryption

Unless otherwise pre-configured on University-owned equipment, users are responsible for performing periodic backups of their mobile devices. Mobile devices are easily lost and frequently stolen, so periodic backups are important.

The backup files created retain the same data classification (Sensitive or Confidential) as the original data and must be stored using an approved medium as described in Section 3.4: Encryption of Data at Rest.

All passcodes used for encryption of files and file systems must meet complexity requirements described in the University’s Password Policy.

Section 5: Prohibited User Actions

5.1: Bypassing Security Mechanisms

In many cases, University-owned devices issued to users will have been pre-configured to adhere to the standards described in this policy. Users must not alter or defeat those pre-configured mechanisms unless expressly instructed to do so by an authorized member of LIT.