Bucknell UNIVERSITY

Mobile and Remote Device Security

Effective Date: February 15, 2018

Summary

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 a path for compromise of other systems.

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.

Scope

This policy applies to any faculty, staff, student, student employee, volunteer or agent of the university who uses a mobile or remote device to access any non-public information systems owned or managed by the University. This policy includes any electronic device that is easily transported and is capable of accessing or storing University information systems or data, including but not limited to laptops, cellular phones, tablets, USB drives (portable and flash based) and CD/DVD media discs regardless of ownership.

Information Security Policy

In order to adequately protect the data and information systems of the University, all individuals covered under this policy are expected to meet the following requirements:

Configuration for Mobile Devices

All users of a mobile electronic device used to access university systems must take the following measures:

- Configure the device to require a password (minimum of 10 characters), biometric identifier, PIN (minimum of 6 characters) or swipe gesture (minimum of 6 swipes) to be entered before local

access to the device is granted. Device must lock and require one of these authentication methods after no more than 5 minutes of idle time.

- Configure the operating system to automatically download and install system patches and updates.
- Ensure that an approved anti-virus package is installed, operational, and configured to automatically download and install signature updates.
- Enable the device's automatic wipe functionality to occur after a sequence of no more than ten unsuccessful attempts to unlock the device.
- Enable the device's remote wipe feature to permit a lost or stolen device to be securely erased.
- Securely store at all times electronic devices to minimize loss via theft or accidental misplacement at all times

Storage of Confidential Data

In general, confidential data should not be stored on mobile devices (including laptops), however, in certain instances depending on job responsibilities, this may be unavoidable. In these instances, data must be stored on university owned devices ONLY with the following requirements:

- Except when being actively used, confidential information must at all times be encrypted on any device through a mechanism approved by the institution.
- Mobile device must have university supported software enabled and running to identify, protect and respond to any threats to the data or operating system of the device.
- Device must have Mobile Device Management software installed to facilitate device protection including remote wipe and device location technology for recovery if possible.

Device Decommission or Separation from University

When mobile devices, specifically personal devices which may have had access to university resources or data that are no longer used, donated, or given to anyone, it is the responsibility of the device owner to ensure any Bucknell information is securely deleted from the device, including Bucknell related e-mail, User ID and Password combinations, or other cached credentials to access Bucknell University systems.

In the event of separation from the University, it is the employee's responsibility to delete any Bucknell related e-mail accounts or Bucknell licensed software that may have been installed on personal devices or computers. For any Bucknell owned equipment, it is expected that it is turned into the appropriate departmental or L&IT services representative on the last day of employment as is required by many of our software licenses and contracts.

Policy Name: Mobile and Remote Device Security		*Policy ID:* IS-004
Related Policies:		
-		
Policy Owner: Chief Information Security Officer		
Policy Reviewed By:		*Next Policy Review Date:*
- General Counsel	Nov/2017	September 2018
- Enterprise Systems Advisory Council	Oct/2017	
- Committee on Library and Information Resources	Oct/2017	