About the Mobile and Remote Device Security Policy

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 and data security.

Information about security breaches from the healthcare industry highlights the potential dangers of using unsecured mobile and remote devices.

> ***Eight of the top ten largest breaches** of medical information – affecting millions of patient records – **were a result of the loss or theft of mobile or remote computing devices**.*

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.

Frequently Asked Questions

Do these policies apply to my personally-owned devices, such as my smartphone or home computer?	**Yes – these policies apply to personally-owned devices.** The University has a responsibility to protect institutional data, no matter where it may exist. As such, personally-owned devices which are used to access University systems must meet the minimum security standards outlined in our policies before they can be used to access or store Sensitive or Confidential information.
With the auto-wipe feature enabled, what safeguards exist against having my phone's data accidentally erased?	**Enabling the auto-wipe feature prevents a malicious user from repeatedly guessing your device's password.** After three to five incorrect guesses, the device will enter a "Disabled" state for a few minutes. Subsequent incorrect attempts cause substantially longer timeout periods, making it very difficult for a malicious user to try a large number of passwords. These timeout periods also prevent the accidental erasure of a device. For example, if a child were using the device, he or she would likely give the phone back after the first timeout period was reached.
Am I required to encrypt my device?	**In most cases, you are not required to encrypt your device.** The encryption requirement applies only to those mobile and remote devices which store Confidential information. University-owned mobile and remote devices, such as laptop computers or portable hard drives, which contain such data for clearly-defined business reasons are required to use full-disk encryption. Since confidential data is not permitted to be stored on any personally-owned devices, there is no requirement for encrypting them.

Securing your mobile devices

Our policies are focused on mitigating the threats to the institution in the event that a mobile device is lost or stolen. In the wrong hands, your device can be used to access any configured accounts and apps, any stored data, or to reveal your Bucknell password to an attacker.

Any mobile device which is used to access or store Confidential or Sensitive University data must meet our baseline security requirements. For smartphones and tablets, these requirements include setting a password on your device and enabling the device's auto-lock and auto-wipe features.

Library and IT (LIT) is responsible for the secure configuration of any University-provided systems, including desktop and laptop computers. For personally-owned computers, our policy states that those systems which access or store Sensitive or Confidential information meet our baseline security requirements as well. These requirements include keeping your system's software up-to-date and, for Windows users, running an appropriate anti-virus software package.

Configuration instructions for your devices can be found below:

Apple iPhone, iPad, or iPod <links to setup documents>
Android
Windows
Macintosh OSX

If you have any questions about securing your remote and mobile devices, please contact the Techdesk at techdesk@bucknell.edu or 570-577-7777.