Berea College

Mobile Device Security Policy
Effective 09/01/2013

Purpose

Berea College manages confidential and sensitive information including personally identifiable information, financial data, personnel records, building plans and more. Some information is protected by federal and state laws or through contractual obligations that restrict use or disclosure. Other information can increase the risk of identity theft if not properly managed. The complexity in protecting this information increases as more mobile devices are connected to campus systems since these devices are small and can be easily lost, stolen, or misplaced. This policy covers the security of College data residing on mobile devices including laptops, smart phones, tablets, e-readers and iPads.

Policy

1. **Password Protection**
   All mobile devices connecting to College services such as email and network storage must have a log-on password enabled that is at least four characters in length. The characters should not be repeating or in sequence (for example do not use 1111, 1234, etc.). Berea's systems are set to require this before you can connect to College email. The device will be configured to lock after no more than fifteen minutes of inactivity and will be automatically wiped after 15 failed attempts to access College email. Employees that do not want to be subject to these requirements can connect their personal devices to Berea's email system using their mobile web browser and connect to http://mail.berea.edu. This mobile interface will not store email, contacts, and calendar items locally on the device.

2. **Sensitive Information**
   Employees are strongly encouraged not to store personally identifiable information, legally-protected data, and sensitive/proprietary information associated with Berea College on mobile devices like smart phones. However, if this is necessary, employees are required to password enable their device. Employees should also avoid storing sensitive College information in their contacts, calendar, or in email folders, if they are using mobile device email features as the information will be automatically transferred to your device.

3. **Lost or Stolen College-owned Mobile Device**
   Employees and students must report a lost or stolen college-owned mobile device immediately to Public Safety at 859-985-3333 and to the Technology Resource Center at 859-985-3343. When applicable, IS&S will issue a remote command to wipe the mobile device to protect college data. The command resets the device to the factory state with all personal data removed. IS&S will also contact the wireless service provider to deactivate the cellular voice capability. As added protection, employees and students can use the Microsoft Outlook Web Interface to issue a wipe command on their own to any mobile device that accesses their email account including personal and college-issued smart phones. Because of these measures, employees issued a college mobile device should keep good backups and consider subscribing to

a tracking service such as ***Find My iPhone***.

4. **Encryption for Positions Handling Sensitive Data**
   Some employees handle particularly sensitive College information. Laptops and mobile devices issued to these employees will have full-disk encryption installed requiring a PIN or Password before the operating system is loaded in order to gain access to applications and data. These PIN's or Passwords should be safeguarded. A backup key code for College-issued laptops will be provided to Public Safety for safekeeping in the event the user forgets the password for the device.

5. **Connecting to College Resources**
   The College does not limit the kind of mobile devices that can be connected to our campus network however, we do reserve the right to block any device or group of devices that place our network, data or other users at risk. This can happen for example when a flawed OS is released on a particular line of mobile devices. Where possible, data transmissions from mobile devices should be encrypted. Some College systems, like email, automatically establish an encrypted connection. Bluetooth and Wi-Fi to the mobile device should be disabled when not in use to prevent unauthorized wireless access.

6. **Disposal of College-owned Mobile Devices**
   All College-owned mobile devices must be returned to the Technology Resource Center in Hutchins when no longer in use or when the employee ceases to work for the College. The TRC will clear data from these units and reissue or recycle the device.

Procedures

1. **Mobile Device End User Agreement**
   This policy is provided to all Mobile Device Users when issued a college mobile device. The form used to request the device, when signed, indicates the user has read and agreed to the terms of this policy. See Policy for Use of Campus-Owned Portable Wireless Devices