Security standards for mobile devices

Introduction:

The IT Security Program APS discusses IT Resource user responsibilities in protecting University data. The purpose of these standards are to provide related acceptable use and security guidance to university employees for protecting university 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

These standards would not apply if the mobile device is just used to browse public information available without any authentication on the university websites. Please contact your campus IT security principal for additional guidance.

Standards:

- Do not store Highly Confidential university data (including sensitive student data, Protected Health Information and Social Security Numbers) on personal mobile devices except when specifically needed for business purposes and approved by the appropriate data owner. Mobile device users who do have a valid business need to store private data must seek guidance regarding additional controls from their campus IT security principal. Additional protection will require encryption of data, the use of passwords, automatic logoffs, and secure Internet transmissions.
- Private university data should never be stored on “jailbroken” or “rooted” devices under any circumstances. Jailbreaking or rooting refers to mechanisms that involve overriding device manufacturer’s controls and permissions. While this process potentially gives users more control over their device, it also leaves the device more vulnerable to malicious apps and infections.
- University employees are expected to secure devices to prevent unauthorized access whenever they are left unattended.
- University employees should provide a notification to the campus IT Help Desk as soon as possible, not exceeding 48 hours, in the event of a lost or stolen device containing university data.
- Mobile devices should have at a minimum a 4 digit PIN to Authenticate and an inactivity timeout of not more than 15 minutes.
- Configure the device for remote location and erase services (such as “Find my iPhone”) so that you can locate or erase your device if it is lost. If you are connecting to your campus Outlook/Exchange service you may be able to remotely wipe your device by logging into your campus Outlook Web Access

(OWA). **Remember, it is your responsibility to restore data should it be necessary to remotely erase your device, so make sure your device is securely backed up.**

- **Personal mobile devices should not be used to photograph patients or health care procedures. Designated hospital equipment should be used instead for such purposes.**
- Data stored on mobile devices should be properly purged of all university information before the device is disposed, donated, or an employee's relationship with the University is terminated.
- Personally owned devices should never be used as a means to avoid compliance with campus or departmental policy.
- Be aware that there may be export control restrictions that apply to travel outside of the United States with laptops or other electronic devices. Check with the campus export control office.

The campuses have the authority to establish more stringent standards as appropriate. Exceptions to University or campus standards are to be documented using Office of Information Security (OIS) risk acceptance process.

Please note that your campus has policies or standards to which you are expected to follow. Please contact your Campus Information Security Officer if you have any related questions. Contact details of Campus Information Security Officer and links to policies are available on the OIS website at https://www.cu.edu/ois

Additional Resources:
CU Boulder
Acceptable use of IT policy

UC Denver/AMC
Responsible computing policy

UCCS
Responsible computing policy