SECURITY BASICS FOR MOBILE DEVICES
UNH IT SECURITY, DECEMBER 2011

Choose brands and models of mobile devices that have the options referenced below. Use all available security options that your device offers:

- Activate automatic locking of the device based on an inactivity time-out, holstering the device, etc.
- Require password to unlock or turn on the device.
- Use good password practices: do not share your password, do not use easily guessed passwords, follow university password policy whenever possible.
- Activate self-erase or self-wipe option following entry of a number of incorrect passwords
- Activate the remote wipe option and learn how to execute it remotely
- Turn on "find my device" type of functionality, if available
- Activate encryption if possible

It is a violation of policy to put restricted or sensitive university information in un-approved off-campus services, such as public cloud based services, that have not been reviewed for security through the standard IT Vendor Contracts Security Questionnaire, and covered by a strong contract that protects university information. Be alert for mobile apps that may use cloud based storage.

Report the loss or theft of a device that is used to access UNH data or services immediately.

- During customary work hours, call 862-4242 for the IT Service Desk.
- After hours, call Police Dispatch, 862-1427
- Ask the Service Desk or Dispatcher to notify IT Security.