UA Mobile Computing Guidelines

These guidelines are intended to provide best practices for those who use mobile devices (such as smartphones or tablets) to access university-related data, applications, email and more. A related *Mobile Device Usage Policy* is available at http://go.uillinois.edu/uamobiledevicepolicy).

1. **Protect Access to the Device**
    a. Always keep the device with you or in a safe location.
    b. Use a password with a minimum of six characters or biometric. "Swipe" authentication and "Image selection" authentication are not recommended.
    c. Do not write down passwords.
    d. Use encryption.
    e. Report lost or stolen devices containing University data to AITS Service Desk promptly so that security professionals can provide you with steps you can take to delete data from your device if needed. (Note that by default, you will not be required to delete data, and you will not be penalized for losing a device).
        i. Urbana-Champaign or Springfield: 217-333-3102
        ii. Chicago: 312-996-4806
        iii. Email: servicedeskaits@uillinois.edu
    f. Configure devices to lock after, at most, ten minutes of inactivity.
    g. Enable tracking on your device to provide its location if it is stolen.
    h. Only connect your device to known wireless networks.

2. **Protect Data Stored on the Device**
    a. Minimize the amount of University-related data stored on the device
    b. Keep personal and University data separate on the device.
    c. Remove all data before disposing of a device, including email, documents, contacts, and other application data. Contact your phone carrier's technical support for further instructions.
    d. Remove University data from all devices before entering an Internal Trade in Arms (ITAR) embargoed country (http://www.pmddtc.state.gov/embargoed_countries/)
    e. Use only University-approved internet (cloud) services for storing University data
    f. Do not share internet (cloud) service accounts used to backup University data
    g. Enable "remote wipe" so that University data or personal information can be erased in the case of a lost or stolen device.

3. **Setup the Device with Security in Mind**
    a. You can install anti-malware software, but realize it might not prevent all virus infections
    b. Before installing any application, verify the permissions the software requires do not put your device at risk. For example, a stopwatch app should not ask for access to your address book.
    c. Only purchase or download software from trusted sources.
    d. "Rooting" or "jailbreaking" devices is not recommended and may introduce security risks.
    e. Disable "auto-complete" for user IDs, passwords, credit card numbers, and any other sensitive information.