Additional Resources

Android Security Information
android.com/security

Apple Security Information
apple.com/business/docs/iOS_Security_Guide.pdf

Mobile Device Security Information
staysafeonline.org

UA Board of Regents Policy
02.07.066. Mobile Device Security
alaska.edu/bor/policy-regulations

UAF University of Alaska Fairbanks
UAA University of Alaska Anchorage
University of Alaska Southeast

For additional information contact your local support center, or the University of Alaska Office of Information Technology via phone at (907) 450-8300 or (800) 478-8226, the web at www.alaska.edu/oit, or email at helpdesk@alaska.edu.

UAF University of Alaska Fairbanks

UAA University of Alaska Anchorage.

University of Alaska Southeast

oit Office of Information Technology

University of Alaska
Many Traditions One Alaska

Mobile Device SECURITY

What You Need to Know

10 Tips for **Mobile Device Security**

Mobile devices, such as smartphones and tablets, function while connected to a wireless data network and allow their user to be in motion. While the compact size of mobile devices makes them extremely useful and convenient, the access they give means that residual data is often left behind. This carries with it a certain risk, so attention to security should be paid. What follows are configuration options meant to reduce some of the risks associated with using mobile devices. For more detailed information visit **https://www.alaska.edu/oit/security**.

1 Configure mobile devices to be secure.

- Enable auto-lock.
- Enable password protection and require passwords.

2 Avoid using auto-complete features to remember usernames or passwords.

- Ensure that browser security settings are configured appropriately.
- Enable remote wipe.
- Ensure that SSL protection is enabled, if available.

3 Connect to secure Wi-Fi networks and disable Wi-Fi when not in use.

- Disable remote access features not in use such as Bluetooth, infrared, or Wi-Fi.
- Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices.
- Configure and enable VPN clients software.
- Avoid joining unknown Wi-Fi networks.

4 Backup your device on a regular basis.

- Use backup software on a desktop or syncing services to insure you have access to data when you may no longer have access to the device or need to restore.
- Configure backups to be encrypted.

5 Use anti-virus programs and configure automatic updates, if possible.

- Install anti-virus software as it becomes available and maintain up-to-date signatures and engines. Alternatively, scan devices periodically by connecting them to a computer with anti-virus software.
- Do not download applications from untrusted sites.
- Check your device's app store for options.

6 Use an encryption solution to keep data safe.

- If confidential data must be accessed or stored using a mobile device, enable encryption options.
- Be aware of the encryption options available for your mobile devices.
- To avoid data storage consider using thin client models so that data is centrally and securely maintained.

7 Update mobile devices frequently. Select the automatic update option, if available.

- Maintain up-to-date software, including operating systems and applications.
- Run only manufacturer approved firmware or operating systems.

8 Take appropriate physical security measures to prevent theft or enable recovery of devices.

- Use tracking software or features.
- Never leave your mobile device unattended.
- Report lost or stolen devices immediately.
- Change any passwords stored on or remembered by the device immediately.
- Remember to back up data on your mobile device on a regular basis.

9 Use appropriate sanitization and disposal procedures for mobile devices.

- Delete all information stored in a device prior to discarding, exchanging, or donating it.
- Inoperable devices should be physically destroyed before disposal.

10 Know how to manage your privacy!

- Always consider the convenience mobile devices provide and balance it against the privacy and security of personal information.
- Use privacy settings to control the information you share and who can see it.
- Consider the impacts of using services that collect and share personal data, like your location.
- If you think an activity is inappropriate to conduct on a mobile device, choose another approach.