BSD Securing an iOS Device

Guideline	GDE-04	Effective Date	10/30/15	Modified Date	10/27/15	Version	1.0

Table of Contents

PURPOSE

The purpose of these guidelines is to ensure greater security on individual assets, specifically for the security of an iOS device.

SCOPE

These guidelines apply to all iOS devices managed by a user.

GUIDELINES

1.0 Computer Settings

Section	Guideline	Guideline Description	Effort Level
1.1	Use a Password	Set a passcode to access your phone. See Apple support https://support.apple.com/en-us/HT204060 for how to set and change a passcode on your iPhone, iPad, or iPod. It is recommended to use a password instead of a 4 digit code.	Low
1.2	Disable Lock Screen Notifications	**Turn** off your lock screen notifications.	Low
1.3	Install and Use Anti-virus Software	You may use your own commercial products.	Medium
1.4	Install and Use a	Set up Find My iPhone. If your device is lost, you can track it or erase the data on it remotely.	Low

	Device Tracking App		
1.5	Encrypt your Mobile Device	See Apple support to enable data protection: https://support.apple.com/en-us/HT202064	High
1.6	**Disable Siri** on Lock Screen	Siri can potentially give away unintended information from the lock screen. Go to Settings>Passcode->Allow access when locked->Siri:off and Settings->General->Siri-> Allow Hey Siri:off.	Low

2.0 Connections

Section	Guideline	Guideline Description	Effort Level
2.1	Use a Secure Internet Connection	Use a secure internet connection. Secure networks include wired connections and uchicago-secure.	Low
2.2	Turn on the UChicago VPN	Install Cisco AnyConnect VPN App if you expect to use untrusted networks (such as guest wireless in a hotel or coffee shop). Go to the App Store search for Cisco AnyConnect click Get and then Install. Start app and OK enabling of the software. Under connections, click Add VPN Connection Enter the Description you would like, and under Server Address enter cvpn.uchicago.edu. Back in the home of the app, swipe right the AnyConnect VPN. Enter your CNetID and Password, enter and Accept the Banner.	Medium
2.3	Turn Off Optional Network Connections	Turn off optional network connections (ie: Wifi, Bluetooth) when not in use. This prevents unauthorized access to your computer through these connections.	Low
2.4	Turn Off iCloud Automatic Sync	Turn off iCloud automatic sync. This prevents involuntary uploading to the cloud, which is often highly insecure.	Low

3.0 Management and Keeping Up-to-date

Section	Guideline	Guideline Description	Effort Level
3.1	Subscribe to the BSD ISO Security Awareness Newsletter List	Bsd_iso-cybersecurity_newsletter@lists.uchicago.edu at lists.uchicago.edu.	Low
3.2	Report	If you use your computer to maintain or access sensitive	Low

	Security Incidents	institutional data and it is lost or stolen, inform your Manager, IT custodian and send an email to the BSD Information Security Office at security@bsd.uchicago.edu.	
3.3	Keep your iOS updated	Turn on automatic updating to keep your iPhone updated This provides you with security updates and other improvements.	Low
3.4	Keep your Applications Updated	Turn on automatic updating for apps to take advantage of security updates and other improvements. Use automatic updating where available to ensure that this happens as needed. Be sure to review an update's effect on the app's ability to access your information.	Low
3.5	Only Install Trusted Applications	Do not download apps offered to you via email, text messages, or web links. Do not install apps offered on pop-ups from third-party websites. If iOS alerts you about an "Untrusted App Developer," click "Don't Trust" on the alert and immediately uninstall the application.	Low
3.6	Do not make Unauthorized Modifications to your iOS	Do not unlock or otherwise bypass security features that prevent you from changing your operating system or downloading unauthorized software. (This hacking process is often called "jailbreaking.")	Low
3.7	Erase Device Securely	Before transferring ownership of an iOS device be sure to erase the devise securely. Go to Settings->General->Reset	Medium
3.8	Be Aware of the Treatment of Confidential Information	Be aware that the University is bound by law or contract to protect some types of confidential information and in other instances the University requires protection of confidential information beyond legal or contractual requirements as an additional safeguard. Refer to http://humanresources.uchicago.edu/fpg/policies/600/p601.shtml.	Low

4.0 Additional Best Practices

Section	Guideline	Guideline Description	Effort Level
4.1	Backup your Data	Always keep a backup copy of files you do not wish to lose. Visit https://www.apple.com/support/iphone/backup/ for more information on how to backup your iOS device.	Low
4.2	Enable Web Browser Security Settings	Choose web browser security settings that protect your privacy and enhance security. Learn more about security features in Safari.	Medium

Resources

- BSD Information Security Office Services
- 601 - Treatment of Confidential Information Policy

Approval and Ownership

Responsible Office: BSD Information Security Office
Guideline Owner: BSD Security Liaison Group

Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	10/27/2015	11/01/2016	BSD SLG Members