BSD Securing an Android Device

Guideline	GDE-03	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 Android device.

SCOPE

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

GUIDELINES

1.0 Computer Settings

Section	Guideline	Guideline Description	Effort Level
1.1	Use a Password	Require the password when your computer sleeps or the screen saver is activated. Do not allow automatic login. In **Settings,** choose **Security,** then **Screen Lock**. In **Screen Lock**, select **Password** and follow the instructions.	Low
1.2	Set a Screensaver	In **Settings**, choose **Security**, then choose **Automatically Lock** and select activation time.	Low
1.3	Install and Use Anti-virus Software	You may use your own commercial products.	Medium
1.4	Install and Use a Device Tracking	Google offers the Android Device Manager (log in to My Devices using your UChicago e-mail address). Commercial applications include Lookout Security and Antivirus, Where's My Droid, SeekDroid AntiTheft &	Low

	App	Security, Cerberus anti theft, and Android Lost. Such an app will help you track or remotely erase your device if it is lost or stolen.	
1.5	Encrypt your Mobile Device	In **Settings,** choose **Security,** then choose **Encrypt phone** and follow the instructions.	Low
1.6	Turn on the built-in firewall	In the **Play Store**, search for and download the **NoRoot Firewall** application. Open the application and allocate permissions for particular applications.	Medium

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 (Virtual Private Network)	Install the Cisco AnyConnect VPN App and Turn on UChicago cVPN if using untrusted wireless networks (ie: coffee shops, guest wifi, most publicly accessible non-password protected wifi). This Cisco AnyConnect VPN app works with most Android devices, however it is not guaranteed to work on all Android devices due to the wide variety of Androids available. Go to the Google Play Store and search for Cisco AnyConnect. Choose the AnyConnect ICS+ app and tap Install. If prompted, tap Accept to give AnyConnect permission to access other apps. Tap Open and accept the license agreement if one is presented. Choose to add a new VPN connection by tapping Connection. If the Advanced Preferences screen displays, tap Add a New VPN Connection. Enter the following information: Description: label the configuration with a unique identifier (for example, UChicago VPN). Server Address: https://cvpn.uchicago.edu. Tap Done. Tap the AnyConnect VPN Off button. When prompted for your username and password, enter your CNetID and Password, and tap Connect. Utilizing the UChicago cVPN provides a secure computing experience when accessing a UChicago network or PHI from a remote location or when using Wi-Fi.	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

3.0 Management and Keeping Up-to-date

Section	Guideline	Guideline Description	Effort Level
3.1	Subscribe to	Bsd_iso-cybersecurity_newsletter@lists.uchicago.edu at	Low

	the BSD ISO Security Awareness Newsletter List	lists.uchicago.edu.	
3.2	Report Security Incidents	If you use your computer to maintain or access sensitive 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.	Low
3.3	Keep your Android OS updated	We recommend that people avoid connecting to UChicago networks from machines running Android 3.2.6 and older.	Low
3.4	Keep your Applications Updated	This is to take advantage of security updates and other improvements. Go to the **Play Store** and find the **My Apps** tab. Follow the instructions and update installed applications.	Low
3.5	Only Install Trusted Applications	Only install trusted market apps, such as Google play apps. To avoid installing malware that may be hiding in untrusted apps.	Low
3.6	Do not make Unauthorized Modifications to your Android	Do not unlock or otherwise bypass device security features that prevent you from gaining privileged control (or "root access") to your device's Android operating system. (This hacking process is often called "rooting."). See Wikipedia's Rooting (Android OS) for more information about the dangers of doing this.	Low
3.7	Erase Device Securely	In **Settings,** choose **Backup & reset,** then choose **Factory data reset** and follow the instructions.	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. In **Settings,** choose **Backup & reset,** then toggle on **Back up my data** and follow the instructions.	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 Firefox and Chrome.	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