Center for Internet Security®

CIS Google Android Benchmark

v1.1.0 - 08-28-2017

Table of Contents

Overview 4
Intended Audience 4
Consensus Guidance 4
Typographical Conventions 5
Scoring Information 5
Profile Definitions 6
Acknowledgements 7
Recommendations 8
1 Android OS Security Settings 8
1.1 Ensure device firmware is up to date (Not Scored) 8
1.2 Ensure 'Screen Lock' is set to Enabled (Not Scored) 10
1.3 Ensure 'Make pattern visible' is set to Disabled (if using a pattern as device lock mechanism) (Not Scored) 12
1.4 Ensure 'Automatically Lock' is set to 'Immediately' (Not Scored) 14
1.5 Ensure 'Power button instantly locks' is set to Enabled (Not Scored) 16
1.6 Ensure 'Lock Screen Message' is configured (Not Scored) 18
1.7 Do not connect to untrusted Wi-Fi networks (Not Scored) 20
1.8 Ensure 'Show passwords' is set to Disabled (Not Scored) 22
1.9 Ensure 'Developer Options' is set to Disabled (Not Scored) 24
1.10 Ensure 'Install unknown apps' is set to Disabled (Not Scored) 26
1.11 Do not root your device (Not Scored) 28
1.12 Ensure 'Smart Lock' is set to Disabled (Not Scored) 30
1.13 Ensure 'Lock SIM card' is set to Enabled (Not Scored) 32
1.14 Ensure 'Find My Device' is set to Enabled (Not Scored) 34
1.15 Ensure 'Automatic date & time' and 'Automatic time zone' are set to Enabled (Not Scored) 36
1.16 Ensure 'Remotely locate this device' is set to Enabled (Not Scored) 38
1.17 Ensure 'Allow remote lock and erase' is set to Enabled (Not Scored) 40
1.18 Ensure 'Scan device for security threats' is set to Enabled (Not Scored) 42
1.19 Ensure 'Improve harmful app detection' is set to Enabled (Not Scored) 44

1.20 Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to Enabled (Not Scored) 46
1.21 Ensure 'Sleep' is set to 1 minute or less (Not Scored) 48
1.22 Ensure 'Wi-Fi assistant' is set to Disabled (Not Scored) 50
1.23 Keep device Apps up to date (Not Scored) 52
1.24 Ensure 'Add users from lock screen' is set to Disabled (Not Scored) 54
1.25 Ensure 'Guest profiles' do not exist (Not Scored) 56
1.26 Review app permissions periodically (Not Scored) 58
1.27 Ensure Wi-Fi hotspot security is set to WPA2-PSK (Not Scored) 60
1.28 Ensure 'Instant apps' is set to Disabled (Not Scored) 62
2 Android OS Privacy Settings 64
2.1 Ensure 'Notifications on the lock screen' is set to Disabled (Not Scored) 64
2.2 Ensure 'Location Services' is set to Disabled (Not Scored) 66
2.3 Ensure 'Back up to Google Drive' is Disabled (Not Scored) 68
2.4 Ensure 'Signed-out search activity' is set to Disabled (Not Scored) 70
2.5 Ensure 'Web and App Activity' is set to Disabled (Not Scored) 72
2.6 Ensure 'Device Information' is set to Disabled (Not Scored) 74
2.7 Ensure 'Voice & Audio Activity' is set to Disabled (Not Scored) 76
2.8 Ensure 'YouTube Search History' is set to Disabled (Not Scored) 78
2.9 Ensure 'YouTube Watch History' is set to Disabled (Not Scored) 80
2.10 Ensure 'Google Location History' is set to Disabled (Not Scored) 82
2.11 Ensure 'Opt out of Ads Personalization' is set to Enabled (Not Scored) 84
Appendix: Summary Table 86
Appendix: Change History 88

Overview

This document, Security Configuration Benchmark for Google Android, provides prescriptive guidance for establishing a secure configuration posture for the Google Android OS. This guide was tested against the Android 8.0.0 OS Build number OPR6.170623.012. This benchmark covers Android 8.x.x and all hardware devices on which this OS is supported.

In determining recommendations, the current guidance treats all Android mobile device platforms as having the same use cases and risk/threat scenarios. In all but a very few cases, configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, end users, and platform deployment personnel who plan to use, develop, deploy, assess, or secure solutions that use Android 8.x.x

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Pravin Goyal, Cavirin Systems, Inc

Editor
Jordan Rakoske GSEC, GCWN

Recommendations

1 Android OS Security Settings

This section provides the security recommendation for Android OS.

1.1 Ensure device firmware is up to date (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the device is kept up to date with security patch levels.

Rationale:

Firmware updates often include critical security fixes that reduce the probability of an attacker remotely exploiting the device. The device should be on the latest security patch level as applicable.

Audit:

To verify that your device is updated to the most recent firmware version:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `System updates`.
4. Verify that the `Android Security patch level` is current and that no new updates exist.

Remediation:

Follow the below steps to check and update the device security patch level:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `System Updates`.
4. Tap `Check for update`.
5. Apply the update, if available.

Impact:

None

Default Value:

By default, users are notified about security patch level updates but are not installed until the user initiates the process.

References:

1. https://source.android.com/security/bulletin/index.html

CIS Controls:

4 Continuous Vulnerability Assessment and Remediation
Continuous Vulnerability Assessment and Remediation

1.2 Ensure 'Screen Lock' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable `Screen lock`.

Rationale:

Enabling `Screen lock` requires a form of user authentication before interacting with the device. This strengthens application and data protection and overall improves the device security.

Audit:

Verify that a Pattern, PIN or Password has been set for the device.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device Security` section.
4. Verify that `Screen lock` has `Pattern`, `PIN` or `Password` underneath the text.

Remediation:

To configure a Pattern, PIN or Password for the device:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device Security` section.
4. Tap `Screen Lock`.
5. Tap `Pattern`, `PIN` or `Password`.
6. Enter a complex Pattern, PIN or Password.
7. Tap `Continue`.
8. Enter in the same complex Pattern, PIN or Password again.
9. Tap `OK`.

Impact:

A user will be prompted to unlock the device on every use.

Default Value:

By default, screen lock is not set.

References:

1. https://support.google.com/nexus/answer/2819522?hl=en&ref_topic=7029556

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.3 Ensure 'Make pattern visible' is set to Disabled (if using a pattern as device lock mechanism) (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable pattern visibility if using a pattern as device lock mechanism.

Rationale:

Keeping device unlock pattern visible during device unlock can reveal the pattern and is vulnerable to shoulder surfing attack. Hence, do not make the device unlock pattern visible.

Audit:

Follow the below steps and verify that device unlock pattern is not visible.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security` section.
4. If `Screen lock` has `Pattern`underneath the text, follow further steps. If not, then this recommendation is not applicable.
5. Tap the `Gear Icon` next to `Screen lock`.
6. Verify that the `Make pattern visible` switch is disabled.

Remediation:

To disable device unlock pattern visibility, follow the below steps:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security` section.
4. If `Screen lock` has `Pattern`underneath the text, follow further steps. If not, then this recommendation is not applicable.
5. Tap the `Gear Icon` next to `Screen lock`.
6. Toggle `Make pattern visible` to Off position.

Impact:

The user would have to be careful while entering the device unlock pattern since visual feedback would not provide any clues for tracing pattern input.

Default Value:

By default, device unlock pattern is visible.

References:

1. https://support.google.com/nexus/answer/2819522?hl=en

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

1.4 Ensure 'Automatically Lock' is set to 'Immediately' (Not Scored)

Profile Applicability:

- Level 1

Description:

Immediately lock the phone as soon as the device goes to sleep.

Rationale:

Automatically and immediately locking the device as soon as it goes to sleep ensure that there is no lag between the device entering the sleep state and the device getting locked. At times, the user just rests the device and moves away from it. The phone eventually enters the sleep state and automatically and immediately locking it ensures that no manual locking of the device is needed. This ensures that the unattended devices are locked immediately as soon as the device enters the sleep state.

Audit:

Follow the below steps and verify that `Automatically Look` is set to `Immediately`.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security` section.
4. Tap the Gear icon next to `Screen lock`.
5. Verify that `Automatically lock` has a text `Immediately after sleep` underneath it.

Remediation:

Follow the below steps and set `Automatically Lock` to `Immediately`.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security` section.
4. Tap the Gear icon next to `Screen lock`.
5. Tap `Automatically lock`.
6. Tap `Immediately`.

Impact:

None

Default Value:

By default, `Automatically lock` is set to 5 seconds after sleep.

CIS Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

1.5 Ensure 'Power button instantly locks' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Pressing the power button should lock the device instantly.

Rationale:

Pressing the power button instantly puts the phone to sleep. Enabling `Power button instantly locks` setting ensures that the device is instantly locked as well.

Audit:

Follow the below steps and verify that `Power button instantly locks` is enabled.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security`.
4. Tap the Gear icon next to `Screen lock`.
5. Verify that `Power button instantly locks` is enabled.

Remediation:

Follow the below steps to enable the `Power button instantly locks` setting.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Device security`.
4. Tap the Gear icon next to `Screen lock`.
5. Toggle `Power button instantly locks` setting to On position.

Impact:

None

Default Value:

By default, `Power button instantly locks` setting is enabled.

References:

1. https://support.google.com/nexus/answer/2819522?hl=en

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.6 Ensure 'Lock Screen Message' is configured (Not Scored)

Profile Applicability:

- Level 1

Description:

Set a message to be displayed on the locked screen.

Rationale:

When device screen is locked, a lock screen message helps to provide

- deterrent warnings,
- device recognition without needing to unlock it and
- most importantly emergency information

Such information could be valuable to both your device security as well as personnel security. It is thus recommended to have a suitable lock screen message.

Audit:

Follow the below steps and verify that `Lock screen message` is set.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`
3. Scroll to the `Device security` section.
4. Tap the Gear icon next to `Screen lock`.
5. Verify that a suitable `Lock screen message` is set.

Remediation:

Follow the below steps to set up a `Lock screen message`.

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`
3. Scroll to the `Device security` section.
4. Tap the Gear icon next to `Screen lock`.
5. Tap `Lock screen message`.
6. Write your message and tap `Save`.

Impact:

Anyone who picks up your device can see your message and emergency information without unlocking your phone.

Default Value:

By default, no message is set.

References:

1. https://support.google.com/nexus/answer/7055029?hl=en&ref_topic=7029556

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.7 Do not connect to untrusted Wi-Fi networks (Not Scored)

Profile Applicability:

- Level 2

Description:

Do not connect to untrusted Wi-Fi networks.

Rationale:

Connecting a device to an open untrusted network through unsecured channels can increase the remote attack surface of the device. Additionally, at present, the cellular data network is a more difficult medium to sniff than Wi-Fi. If you are going to be using public Wi-Fi, using a secure VPN is recommended. In most cases, you should avoid using a public or untrusted or free Wi-Fi.

Audit:

Follow the below steps to verify that `Wi-Fi` is either disabled or not connected to an untrusted network:

1. Tap `Settings` Gear Icon.
2. Tap `Network & Internet`.
3. Verify that the`Wi-Fi` switch is in the Off position or is connected to a trusted network only.

Remediation:

Follow the below steps to disable `Wi-Fi` or connect to a trusted network:

1. Tap `Settings` Gear Icon.
2. Tap `Network & Internet`.
3. Toggle `Wi-Fi` setting to the Off position or connect to a trusted network.

Impact:

You might have to use cellular data and would not be able to take advantage of Public Wi-Fi.

Default Value:

NA

References:

1. https://support.google.com/pixelphone/answer/2819519?hl=en&ref_topic=7084392

CIS Controls:

15.4 Configure Only Authorized Wireless Access On Client Machines
Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

1.8 Ensure 'Show passwords' is set to Disabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable password visibility during input.

Rationale:

This setting controls whether passwords typed into your Android device should be visible on screen, or hidden by replacing the letters with dots. When this setting is off, the password is obscured by dots, and only the most recent key pressed is visible for a short time after it has been pressed. When this setting is on, the entire password can be viewed in plain text, if desired.

Disabling this setting protects you against shoulder surfing attacks.

Audit:

Follow the below steps to verify `Show passwords` is set to disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Privacy` section.
4. Verify that `Show passwords` slider is off.

Remediation:

Follow the below steps to disable `Show passwords`:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to the `Privacy` section.
4. Toggle `Show passwords` to Off position.

Impact:

Given the relative difficulty of typing letters accurately on a small on-screen keyboard, it can be helpful to get visual feedback on-screen that you have typed all the letters of your password correctly. Disabling password visibility might impact user experience.

Default Value:

By default, passwords are visible.

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.9 Ensure 'Developer Options' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable Developer Options.

Rationale:

Enabling `Developer Options` allows a user to drastically alter certain very advanced settings on the device. This can severely affect the way device functions and exposes greater and developmental features to the user. This also exposes the device to respond to features such as USB debugging (when enabled) and other such features that could be exploited to get malicious access to the device sub-system. Hence, the `Developer Options` should be disabled.

Audit:

Follow the below steps to verify that `Developer Options` is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Developer options`.
4. Verify that it is `Off`.

Remediation:

Follow the below steps to disable `Developer Options`:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Developer options`.
4. Toggle it to Off position.

Impact:

None

Default Value:

Bu default, `Developer options` is disabled.

References:

1. http://www.howtogeek.com/175151/8-things-you-can-do-in-androids-developer-options/

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.10 Ensure 'Install unknown apps' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable installation of apps from unknown sources.

Rationale:

This setting determines whether applications can be installed from locations other than Google Play. Disabling installation from untrusted distribution channels protects against inadvertent installation of untrusted or malicious applications. Apps on Google play are vetted by Google Security Team and are mostly safe to install. You should avoid installing apps from anywhere else.

Audit:

Follow the below steps to verify that `Install unknown apps` is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Special app access`.
5. Tap `Install unknown apps`.
6. Verify that all of the apps in the list show `Not allowed`.

Remediation:

Follow the below steps to disable `Install unknown apps`:

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Special app access`.
5. Tap `Install unknown apps`.
6. Tap any app showing `Allowed`.
7. Toggle `Allow from this source` to Off position.

Impact:

None

Default Value:

By default, `Install unknown apps` is disabled.

References:

1. https://support.google.com/nexus/answer/2812853?hl=en

CIS Controls:

2 Inventory of Authorized and Unauthorized Software
Inventory of Authorized and Unauthorized Software

1.11 Do not root your device (Not Scored)

Profile Applicability:

- Level 1

Description:

Do not root your device.

Rationale:

Rooting your Android device breaks the user level restrictions put by the Android operating system. This significantly opens up the device to allow literally any privileged action. Rooting enables any form of alteration to the device. This puts the device at a much greater risk because any vulnerability can be exploited without any restrictions. This also voids the warranty and future security updates are problematic to install. Hence, for all user purposes, do not root your device.

Audit:

Detecting whether a device is rooted or not is not straight forward. You would usually need to install terminal apps or root checker apps to detect rooted devices. Follow your device manufacturer support/documentation/community to detect rooting.

Remediation:

Follow your device manufacturer support/documentation/community to completely un-root your device.

Impact:

None

Default Value:

By default, devices are not rooted and run with user level restrictions.

References:

1. http://www.wikihow.com/Check-if-Your-Android-Cellphone-Is-Rooted-or-Not
2. http://www.wikihow.com/Unroot-Android

CIS Controls:

5 Controlled Use of Administration Privileges
Controlled Use of Administration Privileges

1.12 Ensure 'Smart Lock' is set to Disabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable `Smart Lock`.

Rationale:

`Smart Lock` detects device presence and its circumstances and automatically keeps it unlocked even if the device has a screen password, pin or pattern enabled. Using `Smart Lock` does not require you to manually unlock the device every time if the pre-defined circumstances are met. As a best practice, do not set the device to get unlocked automatically. For example, if your device gets stolen and if it is taken to a location pre-defined in `Smart Lock`, it would automatically unlock. Similarly, if someone could replay your voice, the device would automatically unlock.

Audit:

Follow the below steps to verify that `Smart Lock` is disabled:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Trust agents`.
4. Verify that `Smart Lock (Google)` is Off.

Remediation:

Follow the below steps to disable `Smart Lock`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Trust agents`.
4. Toggle `Smart Lock (Google)` to Off position.

Impact:

The device would need to be manually unlocked everytime.

Default Value:

By default, `Smart Lock` is enabled.

References:

1. https://support.google.com/nexus/answer/6093922?hl=en

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.13 Ensure 'Lock SIM card' is set to Enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Lock SIM card.

Rationale:

If your device uses a SIM card(s), enable SIM card lock. A SIM card PIN locks the SIM and prevents anyone from removing the SIM card from your device and use it on any other device without knowing the PIN. Also, you might choose to store your contacts and messages on the SIM card and thus it is highly recommended that you safeguard this valuable personal data by setting a custom PIN on the SIM card(s).

Note: Only phones that are not locked by the service provider can lock the SIM card.

Audit:

Follow the below steps to verify that `Lock SIM card` is enabled:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `SIM card lock`.
4. Verify that `Lock SIM card` is enabled.
5. If you have more than one SIM card, click on the 2nd SIM card tab and verify that `Lock SIM card` is enabled there as well.

Remediation:

Follow the below steps to enable `Lock SIM card`:

1. Call up your SIM card provider and get the default SIM PIN.
2. Tap the `Settings` Gear Icon.
3. Tap `Security & Location`.
4. Tap `SIM card lock`.
5. Toggle `Lock SIM card` to the on position.
6. Enter the default PIN provided by your SIM provider.
7. Press `OK`.
8. The `Lock SIM card` option will then be enabled.
9. Tap on `Change SIM PIN`.
10. Again provide the default PIN provided (Old PIN) by your SIM card provider.

11. Type your new custom PIN.
12. Re-type your new custom PIN.
13. Press `OK`.
14. Your custom SIM PIN is then set.
15. Repeat the process for your 2nd SIM, if applicable.

Impact:

You would need to remember your SIM card PIN. If you forget your SIM card PIN, you need your SIM card provider support for unlocking the SIM card.

Default Value:

By default, `Lock SIM card` is disabled. Also, the SIM card has a default PIN set by the provider which is usually universally known.

References:

1. https://support.google.com/android-one/answer/6174402?hl=en-GB

CIS Controls:

3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

1.14 Ensure 'Find My Device' is set to Enabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Setup `Find My Device` as a Device Administrator.

Rationale:

If you lose your Android device, you could use `Find My Device` to find your device and also ring, lock, or erase your device data remotely.

Audit:

Follow the below steps to verify that `Find My Device` is enabled:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Device admin apps`.
4. Verify that the `Find My Device` checkbox is checked .

Remediation:

Follow the below steps to enable `Find My Device`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Device admin apps`.
4. Tap `Find My Device`.
5. Tap `Activate this device admin app`.

Impact:

Google may track your device location anytime.

Default Value:

By default, Find My Device is not enabled.

References:

1. https://support.google.com/pixelphone/answer/3265955

CIS Controls:

1 Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Devices

1.15 Ensure 'Automatic date & time' and 'Automatic time zone' are set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable `Automatic date & time`. For this setting to work correctly, `Automatic time zone` setting should also be enabled.

Rationale:

`Automatic date & time` setting fetches the date and time information from the cellular provider and is generally more accurate and reliable than your own managed and set date and time. Accurate date and time could help in forensics, device recovery through Android Device Manager and maintain application and logs in a time-sync manner.

Audit:

Follow the below steps to verify that `Automatic date & time` setting is enabled:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Date & time`.
4. Verify that `Automatic date & time` setting is enabled.
5. Verify that `Automatic time zone` setting is enabled as well.

Remediation:

Follow the below steps to enable `Automatic date & time` and `Automatic time zone` settings:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Date & time`.
4. Toggle `Automatic date & time` setting to On position.
5. Toggle `Automatic time zone` setting to On position.

Impact:

None

Default Value:

By default, `Automatic date & time` and `Automatic time zone` settings are disabled.

References:

1. https://support.google.com/nexus/answer/2841106?hl=en

CIS Controls:

6 Maintenance, Monitoring, and Analysis of Audit Logs
Maintenance, Monitoring, and Analysis of Audit Logs

1.16 Ensure 'Remotely locate this device' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable remotely locating the device.

Rationale:

`Remotely locate this device` setting helps you to track your lost device using `Find My Device`. It must be enabled for improving the recovery possibility of your device.

Audit:

Follow the below steps to verify that `Remotely locate this device` setting is enabled:

1. Tap `Settings` Gear Icon..
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Find My Device` section.
6. Tap `Find My Device`.
7. Verify that `Remotely locate this device` setting is enabled.

Remediation:

Follow the below steps to enable `Remotely locate this device`:

1. Tap `Settings` Gear Icon..
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to `Find My Device` section.
6. Tap `Find My Device`.
7. Toggle `Remotely locate this device` setting to On position.

Impact:

This setting requires you to keep location services enabled all the time. This might be a privacy issue for you.

Default Value:

By default, `Remotely locate this device` setting is enabled.

References:

1. https://support.google.com/accounts/answer/3265955#location
2. https://support.google.com/nexus/answer/6160491?hl=en

CIS Controls:

1 Inventory of Authorized and Unauthorized Devices
Inventory of Authorized and Unauthorized Devices

1.17 Ensure 'Allow remote lock and erase' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Enable remotely locking and erasing the device.

Rationale:

`Allow remote lock and erase` setting helps you to remotely lock your device or erase your data through `Find My Device`. This helps you to safeguard your privacy and protect your data from unsanctioned access.

Audit:

Follow the below steps to verify that `Allow remote lock and erase` setting is enabled:

1. Tap `Settings` Gear Icon..
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Find My Device` section.
6. Tap `Find My Device`.
7. Verify that `Allow remote lock and erase` setting is enabled.

Remediation:

Follow the below steps to enable `Allow remote lock and erase`:

1. Tap `Settings` Gear Icon..
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Find My Device` section.
6. Tap `Find My Device`.
7. Toggle `Allow remote lock and erase` setting to On position.

Impact:

This setting requires you to keep location services enabled all the time. This might be a privacy issue for you.

Default Value:

By default, `Allow remote lock and erase` setting is enabled.

References:

1. https://support.google.com/accounts/answer/3265955#location
2. https://support.google.com/nexus/answer/6160491?hl=en

CIS Controls:

13 Data Protection
Data Protection

1.18 Ensure 'Scan device for security threats' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Scan device for security threats.

Rationale:

`Scan device for security threats` setting lets Google regularly check your device and prevent or warn about potential harm. This should be always enabled.

Audit:

Follow the below steps to verify that `Scan device for security threats` setting is enabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Security Status` section.
6. Tap `Google Play Protect`.
7. Verify that `Scan device for security threats` setting is enabled.

Remediation:

Follow the below steps to enable `Scan device for security threats`:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Security Status` section.
6. Tap `Google Play Protect`.
7. Toggle `Scan device for security threats` setting to On position.

Impact:

None

Default Value:

By default, `Scan device for security threats` setting is disabled.

References:

1. https://support.google.com/nexus/answer/2812853?hl=en

CIS Controls:

8 Malware Defenses
Malware Defenses

1.19 Ensure 'Improve harmful app detection' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Improve detection of harmful apps.

Rationale:

Enabling `Improve harmful app detection` setting sends anonymous information to Google about apps that were not installed from Google Play. This is especially true if you choose to install apps from "Unknown sources" outside of the Google Play Store. This information helps Google better protect everyone from harmful apps.

Audit:

Follow the below steps to verify that `Improve harmful app detection` setting is enabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Security Status` section.
6. Tap `Google Play Protect`.
7. Verify that `Improve harmful app detection` setting is enabled.

Remediation:

Follow the below steps to enable `Improve harmful app detection`:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Security`.
5. Scroll to the `Security Status` section.
6. Tap `Google Play Protect`.
7. Toggle `Improve harmful app detection` setting to On position.

Impact:

User data needs to be sent to Google that may incur data charges based on your carrier. Also, this user data might contain, but not restricted to, log information, URLs related to the app, device ID, your Android version, and IP address.

Default Value:

By default, `Improve harmful app detection` setting is disabled.

References:

1. https://support.google.com/nexus/answer/2812853?hl=en

CIS Controls:

8 Malware Defenses
Malware Defenses

1.20 Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Unpinning should require re-authentication.

Rationale:

Your might lend your device to a friend or anyone else for carrying out a single task such as make an emergency phone call or play a game. You should use screen pinning in such a situation. It locks the users to the particular screen that you handed over the device with. Users cannot use the device outside of that application until the screen is unpinned. Unpinning screen should require re-authentication.

Audit:

Follow the below steps to verify that `Ask for pattern/PIN/password before unpinning` setting is enabled:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Screen pinning`.
4. If `Screen Pinning` is `On`, then verify that `Ask for pattern/PIN/password before unpinning` setting is enabled.

Remediation:

Follow the below steps to enable `Ask for pattern/PIN/password before unpinning`:

1. Tap the `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Tap `Screen pinning`.
4. If you are using `Screen Pinning`, then toggle `Ask for pattern/PIN/password before unpinning` setting to On position.

Impact:

None

Default Value:

By default, if you enable `Screen pinning`, then `Ask for pattern/PIN/password before unpinning setting` is also enabled if you have previously chosen to lock your device with a pattern, PIN or password. If you have previously chosen to not lock your device, you would be required to set it up by tapping `Lock device when unpinning` after enabling `Screen pinning`.

References:

1. https://support.google.com/nexus/answer/6118421?hl=en&ref_topic=7029159

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.21 Ensure 'Sleep' is set to 1 minute or less (Not Scored)

Profile Applicability:

- Level 1

Description:

Set `Sleep` setting to 1 minute of less.

Rationale:

You should set inactivity timeout to avoid unsanctioned usage of the device if you leave it unattended. The inactivity timeout not only blackens your screen after stipulated time period but also kicks in other security features such as screen lock that protect your device when you leave it unattended.

Audit:

Follow the below steps to verify that `Sleep` setting is set to 1 minute or less:

1. Tap on `Settings` Gear Icon.
2. Tap `Display`.
3. Tap `Advanced`.
4. Verify that `Sleep` is set to 1 minute or less.

Remediation:

Follow the below steps to set `Sleep` setting to 1 minute or less:

1. Tap on `Settings` Gear Icon.
2. Tap `Display`.
3. Tap `Advanced`.
4. Tap `Sleep`.
5. Tap on time duration of 1 minute or less.

Impact:

You would need to unlock your device after every time inactivity period is reached.

Default Value:

By default, `Sleep` is set to 1 minute of inactivity.

References:

1. https://support.google.com/pixelphone/answer/6111557

CIS Controls:

16.4 Automatically Log Off Users After Standard Period Of Inactivity
Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

1.22 Ensure 'Wi-Fi assistant' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable automatically connecting your device to open Wi-Fi.

Rationale:

Wi-Fi assistant automatically connects to any open Wi-Fi and tunnel the connection through Google VPN servers. Even with the level of security included when this setting is enabled, it is recommended that users only connect to trusted networks manually and to leave this setting disabled.

Audit:

Follow the below steps to verify that `Wi-Fi assistant` is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Networking`.
5. Verify that `Wi-Fi assistant` is turned off.

Remediation:

Follow the below steps to disable `Wi-Fi assistant`:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Networking`.
5. Toggle `Wi-Fi assistant` to Off position.

Impact:

You would not benefit from open Wi-fi connections and would require using cellular data.

Default Value:

By default, `Wi-Fi assistant` setting is enabled.

Note: on the Verizon Variant this setting is disabled. Also, this feature is available only on Pixel phones and Nexus devices running Android 5.1 and up in the selected countries.

References:

1. https://support.google.com/nexus/answer/6327199?hl=en

CIS Controls:

15.4 Configure Only Authorized Wireless Access On Client Machines
Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

1.23 Keep device Apps up to date (Not Scored)

Profile Applicability:

- Level 1

Description:

Regularly update your device apps.

Rationale:

Keeping apps updated gives you access to the latest features and improves app security and stability. This has similar advantages as patching. Hence, keep your device apps updated.

Audit:

Follow the below steps to verify that Apps are up to date:

1. Tap/slide up `Launcher`.
2. Launch `Play Store` App in the App drawer.
3. Tap `Menu`.
4. Tap `My apps & Games`.
5. Verify that all apps are up to date.

Remediation:

Follow the below steps to update all Apps:

1. Tap/slide up `Launcher`.
2. Launch `Play Store` App in the App drawer.
3. Tap `Menu`.
4. Tap `My apps & Games`.
5. If there are any updates pending, then tap `Update All`.

Impact:

You might incur data charges.

Default Value:

By default, apps are automatically updated. If cellular data is not a concern or secure Wi-Fi is available then you can leave the default Playstore app setting to auto update the apps to ensure that apps are updated automatically.

References:

1. https://support.google.com/googleplay/answer/113412?hl=en-IN

CIS Controls:

4 Continuous Vulnerability Assessment and Remediation
Continuous Vulnerability Assessment and Remediation

1.24 Ensure 'Add users from lock screen' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Do not allow adding users on a locked device.

Rationale:

Users and the guest profile can do most of the same things as the device's owner, but each profile has its own storage space. Guests could install malicious apps or carry out any other malicious activities that may compromise overall device security. Also, Wi-Fi and Bluetooth connections are shared which could give guests unauthorized access to networks/devices that could compromise data. Hence, `Add users from lock screen` setting should be disabled.

Audit:

Follow the below steps to verify that `Add users from lock screen` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Users & accounts`.
3. Verify that `Add users from lock screen` setting is disabled.

Remediation:

Follow the below steps to disable `Add users from lock screen` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Users & accounts`.
3. Toggle `Add users from lock screen` setting to Off position.

Impact:

Users will not be able to add additional users when the device is locked.

Default Value:

By default, `Add users from lock screen` setting is enabled.

References:

1. https://support.google.com/pixelphone/answer/2865944

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

1.25 Ensure 'Guest profiles' do not exist (Not Scored)

Profile Applicability:

- Level 1

Description:

Do not add any guest profiles on the device.

Rationale:

Users and the guest profile can do most of the same things as the device's owner, but each profile has its own storage space. Guests could install malicious apps or carry out any other malicious activities that may compromise overall device security. Also, Wi-Fi and Bluetooth connections are shared which could give guests unauthorized access to networks/devices that could compromise data. Hence, do not add any guest profiles on the device.

If you need to give your device to someone for temporary use, use `Screen Pinning` to restrict access to the desired app and be in the complete visibility of your device all the time.

Audit:

Follow the below steps to verify that the `Guest profile` do not exist:

1. Tap `Settings` Gear Icon.
2. Tap `Users & accounts`.
3. Tap `Users`.
4. Verify that `Guests` is grayed out.

Remediation:

Follow the below steps remove the `Guest profile`:

1. Open `Quick Settings` drawer.
2. Tap the `Profile` icon.
3. Switch to `Guest profile`.
4. Open `Quick Settings` drawer.
5. Tap `Remove guest`.
6. Confirm removal by tapping `remove`.

Impact:

None

Default Value:

By default, `Guest profiles` do not exist.

References:

1. https://support.google.com/pixelphone/answer/2865944
2. https://support.google.com/pixelphone/answer/6115141?hl=en&ref_topic=7083408

CIS Controls:

16 Account Monitoring and Control
Account Monitoring and Control

1.26 Review app permissions periodically (Not Scored)

Profile Applicability:

- Level 1

Description:

Review your device app's permissions periodically.

Rationale:

App permissions allow you to control which capabilities or information apps could access on your device. This can extend from using device hardware to using your personal data. You should periodically review your all app's permissions and ensure that those apps have legitimate permissions. Uninstall apps that over-seek permissions.

Audit:

Follow the below steps to review your app permissions:

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `App permissions`.
4. Tap on each permission and review the apps that have them.
5. After you have carried out the above steps, come back and scroll to `Additional permissions`.
6. Tap `Additional permissions`.
7. Tap on each permission and review the apps that have them.

Remediation:

Follow the below steps to set your app permissions appropriately:

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `App permissions`.
4. Tap on each permission and review the apps that have them.
5. Disable the app permissions that you feel are over-permissive.
6. After you have carried out the above steps, come back and scroll to `Additional permissions`.
7. Tap `Additional permissions`.
8. Tap on each permission and review the apps that have them.
9. Disable the app permissions that you feel are over-permissive.

Impact:

Some of the apps tend to have more than required permissions. Such apps might not work if you disable the permissions it originally asked for. Also, if you disable the needed permissions, you may not be able to use the app and might have to re-install it.

Default Value:

By default, apps seek permissions on first use or during installation.

References:

1. https://support.google.com/googleplay/answer/6270602?hl=en-IN

CIS Controls:

14.4 Protect Information With Access Control Lists
All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.

1.27 Ensure Wi-Fi hotspot security is set to WPA2-PSK (Not Scored)

Profile Applicability:

- Level 1

Description:

Secure your Wi-Fi hotspot with WPA2-PSK.

Rationale:

You could set up a Wi-Fi hotspot on your device. Securing it with `WPA2-PSK` ensures that the connection to this Wi-Fi hotspot could be established only with a password and the data is encrypted in transit. Using WPA2-PSK, the wireless access point uses the common passphrase to generate unique encryption keys for each wireless client. If you set security to `None`, the Wi-Fi hotspot does not require any authentication and all data could be possibly captured.

Audit:

Follow the below steps to verify that Wi-Fi hotspot security is set to WPA2-PSK:

1. Tap on `Settings` Gear Icon.
2. Tap `Network & Internet`.
3. Tap `Hotspot & tethering`.
4. Tap `Set up Wi-Fi hotspot`.
5. Verify that `Security` setting is set to `WPA2-PSK`.

Remediation:

Follow the below steps to set Wi-Fi hotspot security to WPA2-PSK:

1. Tap on `Settings` Gear Icon.
2. Tap `Network & Internet`.
3. Tap `Hotspot & tethering`.
4. Tap `Set up Wi-Fi hotspot`.
5. Tap `Security` setting and set it to `WPA2-PSK`.
6. Choose the desired `Password`.
7. Tap `Save`.

Impact:

None

Default Value:

By default, Wi-Fi hotspot security is set to `WPA2-PSK`.

References:

1. https://support.google.com/fi/answer/6182204
2. https://support.google.com/nexus/answer/2812516
3. https://stage.juniper.net/techpubs/en_US/junos-space-apps12.3/network-director/topics/concept/wireless-wpa-psk-authentication.html

CIS Controls:

15.5 Protect All Wireless Traffic with AES and WPA2
Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

1.28 Ensure 'Instant apps' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable instant apps.

Rationale:

Instant apps allow you to use apps without installing them on your device. On clicking app links, the browser downloads and run app modules as desired by the user.

Having exposure to an app like this is dangerous since any malicious link could then potentially trick the user and then browser could download the app code and run on your device without requiring installation. Also, this feature defies enterprise security that relies on blacklisting or whitelisting apps based on installation. Hence, it is recommended to turn off instant apps.

Audit:

Follow the below steps to verify that `Instant apps` is disabled:

1. Tap on `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Default apps`.
5. Tap `Opening links`.
6. Verify that `Instant apps` setting is set to Off position.

Remediation:

Follow the below steps to disable `Instant apps`:

1. Tap on `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Advanced`.
4. Tap `Default apps`.
5. Tap `Opening links`.
6. Toggle `Instant apps` setting to Off position.

Impact:

Instant apps will not be available. The app links would open on the browser as other regular links.

Default Value:

By default, `Instant apps` is enabled.

References:

1. https://support.google.com/googleplay/answer/7240211
2. https://www.appthority.com/mobile-threat-center/blog/will-googles-instant-apps-undermine-enterprise-security/
3. https://developer.android.com/topic/instant-apps/index.html

CIS Controls:

18 Application Software Security
Application Software Security

2 Android OS Privacy Settings

This section provides the privacy-related recommendation for Android OS.

2.1 Ensure 'Notifications on the lock screen' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable notifications on the lock screen.

Rationale:

If the device is lost or is unattended, then disabling notifications do not display any notification information on the locked screen. This information might be private or confidential and thus unwarranted disclosures could be avoided.

Audit:

To verify Notifications `on the lock screen` are set to `Don't show notifications at all`:

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Notifications`.
4. Verify that `On the lock screen` is set to `Don't show notifications at all`.

Remediation:

Follow the below steps to set the On the lock screen to `Don't show notifications at all`.

1. Tap `Settings` Gear Icon.
2. Tap `Apps & notifications`.
3. Tap `Notifications`.
4. Tap `On the lock screen` and set it to `Don't show notifications at all`.

Impact:

The user will not be able to see contents of notifications on lock screen requiring her to unlock the device each time.

Default Value:

By default, notification content is shown on the locked screen.

References:

1. https://support.google.com/pixelphone/answer/6111294?hl=en&ref_topic=7078221

CIS Controls:

16.5 Ensure Workstation Screen Locks Are Configured
Configure screen locks on systems to limit access to unattended workstations.

2.2 Ensure 'Location Services' is set to Disabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable Location Services when not in use.

Rationale:

Location Services allows applications such as Maps and Internet websites to gather and use data indicating the user's location. The user's location is determined using available information from cellular network data, local Wi-Fi networks, Bluetooth and GPS. If the user turns off Location Services, the user will be prompted to turn it back on again the next time any application tries to use this feature.

Disabling location services reduces the capability of an attacker to determine or track the user's location via websites, locally installed applications or other means without user's consent. Thus, it should be disabled when not in use.

Note: Location service is very important for tracking your lost device if the device data is not disabled. Make a judicious call and decide what works best for you or in your environment.

Audit:

Follow the below steps to verify that `Location services` is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to `Privacy`.
4. Tap `Location`.
5. Verify that `Location` is OFF.

Remediation:

Follow the below steps to disable `Location Services`:

1. Tap `Settings` Gear Icon.
2. Tap `Security & Location`.
3. Scroll to `Privacy`.
4. Tap `Location`.

5. Toggle to the Off position.

Impact:

Each time an application needs location data, the user activity would be interrupted to enable the location services.

Another impact could be on finding your lost device. If the device is lost and the location services are disabled, you cannot use remote locate services such as Android Device Manager.

Default Value:

By default, Location Services is enabled.

References:

1. https://support.google.com/pixelphone/answer/3467281?hl=en&ref_topic=7083817

CIS Controls:

13 Data Protection
Data Protection

2.3 Ensure 'Back up to Google Drive' is Disabled (Not Scored)

Profile Applicability:

- Level 2

Description:

Disable Backup to Google Drive.

Rationale:

You can back up content, data, and settings from your device to your Google Account. You can then later restore your backed-up information to another device. Due to privacy concerns, backing up personal data such as text messages, emails, photos and contacts to any third party is not recommended unless you accept the risk of sharing the data with the 3rd party. Moreover, if you are using a personal device for business apps such as emails, that data might be backed up as well in the Google Drive related to your personal account and might be exposed. Hence, disable the automatic backup to Google drive and carefully choose what data backup you need.

Audit:

Follow the below steps to verify `Back up to Google Drive` is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Backup`.
4. Verify that `Back up to Google Drive` is `Off`.

Remediation:

Follow the below steps to disable `Back up to Google Drive`:

1. Tap `Settings` Gear Icon.
2. Tap `System`.
3. Tap `Backup`.
4. Tap `Back up to Google Drive`.
5. Toggle it to Off position.
6. Tap `OK` on warning popup.

Impact:

A backup of the device will not be taken and hence restoration would not be possible. Also, the user would have to carefully choose the data to be backed up and manually back it up periodically.

Default Value:

By default, `Back up to Google Drive` is disabled.

References:

1. https://support.google.com/pixelphone/answer/7179901?hl=en

CIS Controls:

13 Data Protection
Data Protection

2.4 Ensure 'Signed-out search activity' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable linking your searches to your account when logged out.

Note: This setting is not applicable for Google Pixel range of devices.

Rationale:

`Signed-out search activity` setting controls if your searches on the device are linked to your account even if you are logged out. If you keep this setting enabled, your search results are tweaked to list more personalized results even if you are logged out. This is a form of activity and profile building and might be privacy-invasive. It is recommended that you turn this off.

Audit:

Follow the below steps to verify that `Signed-out search activity` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Account`.
8. Verify that `Signed-out search activity` setting is disabled.

Remediation:

Follow the below steps to disable `Signed-out search activity`:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Account`.
8. Toggle `Signed-out search activity` setting to Off position.

Impact:

You will not get personalized search results when you are logged out.

Default Value:

By default, `Signed-out search activity` setting is enabled.

References:

1. http://www.techgainer.com/disable-prevent-google-web-search-history/
2. https://support.google.com/nexus/answer/54068?co=GENIE.Platform%3DAndroid&hl=en

CIS Controls:

13 Data Protection
Data Protection

2.5 Ensure 'Web and App Activity' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable linking of web and app activity to your account when you are logged out.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

When this setting is enabled, your searches and activity from other Google services are linked and saved to your Google Account, even when you are logged out or offline. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `Web & App Activity` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `Web & App Activity` setting is disabled.

Remediation:

Follow the below steps to disable `Web & App Activity` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Toggle `Web & App Activity` setting to Off position.

Impact:

Web and App activities would not be linked to your account. You might not get personalized user experience.

Default Value:

By default, `Web & App Activity` is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/websearch/answer/54068

CIS Controls:

13 Data Protection
Data Protection

2.6 Ensure 'Device Information' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing device information to your account.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

Turning on `Device Information` setting saves various device related information to your account to give you personalized results, suggestions, and experiences. The information saved might include contact lists, calendars, alarms, apps, and music. Additionally, information such as whether the screen is on, the battery level, the quality of your Wi-Fi or Bluetooth connection, touchscreen and sensor readings, and crash reports are also saved and shared with Google. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `Device Information` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `Device Information` setting is disabled.

Remediation:

Follow the below steps to disable `Device Information` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.

6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Toggle `Device Information` setting to Off position.

Impact:

You might not get personalized user experience.

Default Value:

By default, `Device Information` is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/accounts/answer/6135999

CIS Controls:

13 Data Protection
Data Protection

2.7 Ensure 'Voice & Audio Activity' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable saving your voice and other audio to your Google Account.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

Google records your voice and other audio when you use audio activations. Audio can be saved even when your device is offline. When Voice & Audio Activity is off, voice inputs won't be saved to your Google Account, even if you're signed in. Instead, they may only be saved using anonymous identifiers. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `Voice & Audio Activity` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `Voice & Audio Activity` setting is disabled.

Remediation:

Follow the below steps to disable `Voice & Audio Activity` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Toggle `Voice & Audio Activity` setting to Off position.

Impact:

You might not get personalized user experience.

Default Value:

By default, `Voice & Audio Activity` setting is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/websearch/answer/6030020

CIS Controls:

13 Data Protection
Data Protection

2.8 Ensure 'YouTube Search History' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Search History to your account.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

Turning on `YouTube Search History` setting links and stores all your YouTube searches to your account across any device. Also, your YouTube and Google search history influences the recommendations that you see on your YouTube homepage when you are logged-in. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `YouTube Search History` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `YouTube Search History` setting is disabled.

Remediation:

Follow the below steps to disable `YouTube Search History` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Toggle `YouTube Search History` setting to Off position.

Impact:

You might not get personalized user experience.

Default Value:

By default, `YouTube Search History` setting is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/youtube/answer/57711

CIS Controls:

13 Data Protection
Data Protection

2.9 Ensure 'YouTube Watch History' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing YouTube Watch History to your account.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

Turning on `YouTube Watch History` setting links and stores all your watched YouTube videos to your account from any device. Also, this influences the recommendations that you see on your YouTube homepage when you are logged-in and other YouTube video recommendations. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `YouTube Watch History` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `YouTube Watch History` is disabled.

Remediation:

Follow the below steps to disable `YouTube Watch History` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Toggle `YouTube Watch History` setting to Off position.

Impact:

You might not get personalized user experience.

Default Value:

By default, `YouTube Watch History` setting is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/youtube/answer/95725

CIS Controls:

13 Data Protection
Data Protection

2.10 Ensure 'Google Location History' is set to Disabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Disable storing your location history.

Note: This setting is applicable only for Google Pixel range of devices.

Rationale:

When `Google Location History`setting is turned on, your device periodically sends diagnostics information to Google about what's working and what's not working in relation to Location History. Location History allows Google to regularly obtain location data from the device. It also stores your Location History to provide results and recommendations across Google products. This could be privacy-invasive and hence it is recommended to disable this setting.

Audit:

Follow the below steps to verify that `Google Location History` setting is disabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.
7. Tap `Google Activity Controls`.
8. Verify that `Google Location History` setting is turned off.

Remediation:

Follow the below steps to disable `Google Location History` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Search`.
5. Scroll to the `Search` section.
6. Tap `Accounts & privacy`.

7. Tap `Google Activity Controls`.
8. Toggle `Google Location History` setting to Off position.

Impact:

You might not get personalized user experience.

Default Value:

By default, `Google Location History` setting is enabled.

References:

1. https://support.google.com/pixelphone/answer/6139018?co=GENIE.Platform%3DDesktop&hl=en
2. https://support.google.com/accounts/answer/3118687

CIS Controls:

13 Data Protection
Data Protection

2.11 Ensure 'Opt out of Ads Personalization' is set to Enabled (Not Scored)

Profile Applicability:

- Level 1

Description:

Restrict apps from building your app profile.

Rationale:

Apps can use your app/browsing data to build a profile for displaying personalized ads. To protect your privacy, you should disable building your profiles from various app/browsing activities.

Audit:

Follow the below steps to verify that `Opt out of Ads Personalization` setting is enabled:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Ads`.
5. Verify that `Opt out of Ads Personalization` setting is turned on.

Remediation:

Follow the below steps to enable `Opt out of Ads Personalization` setting:

1. Tap `Settings` Gear Icon.
2. Tap `Google`.
3. Scroll to the `Services` section.
4. Tap `Ads`.
5. Toggle `Opt out of Ads Personalization` setting to on position.

Impact:

You might not get personalized ads experience.

Default Value:

By default, `Opt out of Ads Personalization` setting is disabled.

References:

1. https://support.google.com/ads/answer/2662922?hl=en

CIS Controls:

13 Data Protection
Data Protection

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Android OS Security Settings**		
1.1	Ensure device firmware is up to date (Not Scored)	☐	☐
1.2	Ensure 'Screen Lock' is set to Enabled (Not Scored)	☐	☐
1.3	Ensure 'Make pattern visible' is set to Disabled (if using a pattern as device lock mechanism) (Not Scored)	☐	☐
1.4	Ensure 'Automatically Lock' is set to 'Immediately' (Not Scored)	☐	☐
1.5	Ensure 'Power button instantly locks' is set to Enabled (Not Scored)	☐	☐
1.6	Ensure 'Lock Screen Message' is configured (Not Scored)	☐	☐
1.7	Do not connect to untrusted Wi-Fi networks (Not Scored)	☐	☐
1.8	Ensure 'Show passwords' is set to Disabled (Not Scored)	☐	☐
1.9	Ensure 'Developer Options' is set to Disabled (Not Scored)	☐	☐
1.10	Ensure 'Install unknown apps' is set to Disabled (Not Scored)	☐	☐
1.11	Do not root your device (Not Scored)	☐	☐
1.12	Ensure 'Smart Lock' is set to Disabled (Not Scored)	☐	☐
1.13	Ensure 'Lock SIM card' is set to Enabled (Not Scored)	☐	☐
1.14	Ensure 'Find My Device' is set to Enabled (Not Scored)	☐	☐
1.15	Ensure 'Automatic date & time' and 'Automatic time zone' are set to Enabled (Not Scored)	☐	☐
1.16	Ensure 'Remotely locate this device' is set to Enabled (Not Scored)	☐	☐
1.17	Ensure 'Allow remote lock and erase' is set to Enabled (Not Scored)	☐	☐
1.18	Ensure 'Scan device for security threats' is set to Enabled (Not Scored)	☐	☐
1.19	Ensure 'Improve harmful app detection' is set to Enabled (Not Scored)	☐	☐
1.20	Ensure 'Ask for unlock pattern/PIN/password before unpinning' is set to Enabled (Not Scored)	☐	☐
1.21	Ensure 'Sleep' is set to 1 minute or less (Not Scored)	☐	☐
1.22	Ensure 'Wi-Fi assistant' is set to Disabled (Not Scored)	☐	☐
1.23	Keep device Apps up to date (Not Scored)	☐	☐
1.24	Ensure 'Add users from lock screen' is set to Disabled (Not Scored)	☐	☐
1.25	Ensure 'Guest profiles' do not exist (Not Scored)	☐	☐
1.26	Review app permissions periodically (Not Scored)	☐	☐

1.27	Ensure Wi-Fi hotspot security is set to WPA2-PSK (Not Scored)	☐	☐
1.28	Ensure 'Instant apps' is set to Disabled (Not Scored)	☐	☐
2	**Android OS Privacy Settings**		
2.1	Ensure 'Notifications on the lock screen' is set to Disabled (Not Scored)	☐	☐
2.2	Ensure 'Location Services' is set to Disabled (Not Scored)	☐	☐
2.3	Ensure 'Back up to Google Drive' is Disabled (Not Scored)	☐	☐
2.4	Ensure 'Signed-out search activity' is set to Disabled (Not Scored)	☐	☐
2.5	Ensure 'Web and App Activity' is set to Disabled (Not Scored)	☐	☐
2.6	Ensure 'Device Information' is set to Disabled (Not Scored)	☐	☐
2.7	Ensure 'Voice & Audio Activity' is set to Disabled (Not Scored)	☐	☐
2.8	Ensure 'YouTube Search History' is set to Disabled (Not Scored)	☐	☐
2.9	Ensure 'YouTube Watch History' is set to Disabled (Not Scored)	☐	☐
2.10	Ensure 'Google Location History' is set to Disabled (Not Scored)	☐	☐
2.11	Ensure 'Opt out of Ads Personalization' is set to Enabled (Not Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
1-24-17	1.0.0	Initial Release
8-28-17	1.1.0	ADDED - 1.28 Ensure 'Instant apps' is set to Disabled. Ticket # 5386
8-28-17	1.1.0	ADDED - CIS Controls Mappings to all recommendations.
8-28-17	1.1.0	ADDED - 2.11 Ensure 'Opt out of Ads Personalization' is set to Enabled. Ticket # 5383
8-28-17	1.1.0	MODIFIED- Updated all recommendation steps to conform to 8.0.0
8-28-17	1.1.0	REMOVED - 1.9 Ensure 'Encrypt phone' or 'Encrypt tablet' is set to Enabled.
8-28-17	1.1.0	REMOVED - Ensure 'Speak passwords' is set to Disabled.