CIS Apple iPadOS 18 Benchmark

v1.0.0 - 10-07-2024

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (CISLegal@cisecurity.org) and request guidance on copyright usage.

NOTE: It is *NEVER* acceptable to host a CIS Benchmark in *ANY* format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the CIS Benchmarks™ are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All CIS Benchmarks™ are available free for non-commercial use from the [CIS Website](#). They can be used to *manually* assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

> **NOTE**: Some tooling focuses only on the CIS Benchmarks™ Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed, since all are important for properly securing systems and are typically in scope for audits.

In addition, CIS has developed CIS [Build Kits](#) for some common technologies to assist in applying CIS Benchmarks™ Recommendations.

When remediating systems (changing configuration settings on deployed systems as per the CIS Benchmarks™ Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

1. **NEVER** deploy a CIS Build Kit, or any internally developed remediation method, to production systems without proper testing.
2. Proper testing consists of the following:

a. Understand the configuration (including installed applications) of the targeted systems.

b. Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.

c. Test the configuration changes on representative lab system(s). This way if there is some issue it can be resolved prior to deploying to any production systems.

d. When confident, initially deploy to a small sub-set of users and monitor closely for issues. This way if there is some issue it can be resolved prior to deploying more broadly.

e. When confident, iteratively deploy to additional groups and monitor closely for issues until deployment is complete. This way if there is some issue it can be resolved prior to continuing deployment.

NOTE: CIS and the CIS Benchmarks™ development communities in CIS WorkBench do their best to test and have high confidence in the Recommendations, but they cannot test potential conflicts with all possible system deployments. Known potential issues identified during CIS Benchmarks™ development are documented in the Impact section of each Recommendation.

By using CIS and/or CIS Benchmarks™ Certified tools, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document, Security Configuration Benchmark for Apple iPadOS 18, provides prescriptive guidance for establishing a secure configuration posture for both Apple iPadOS version 18. This guide was tested against Apple iPadOS 18.0 using Apple Configurator v2.16. This benchmark covers Apple iPadOS 18 on all supported devices. As of the publication of these guidelines, devices supported by iPadOS 18 include the following:

- iPad (6th generation)
- iPad (7th generation)
- iPad (8th generation)
- iPad (9th generation)
- iPad (10th generation)
- iPad Air (3rd generation)
- iPad Air (4th generation)
- iPad Air (5th generation)
- iPad Air (6th generation) 11-inch
- iPad Air (6th generation) 13-inch
- iPad Mini (5th generation)
- iPad Mini (6th generation)
- iPad Pro 10.5-inch
- iPad Pro 12.9-inch (2nd generation)
- iPad Pro 11-inch (1st generation)
- iPad Pro 12.9-inch (3rd generation)
- iPad Pro 11-inch (2nd generation)
- iPad Pro 12.9-inch (4th generation)
- iPad Pro 11-inch (3rd generation)
- iPad Pro 12.9-inch (5th generation)
- iPad Pro 11-inch (4th generation)
- iPad Pro 12.9-inch (6th generation)
- iPad Pro 11-inch (5th generation)
- iPad Pro 13-inch (7th generation)

The current guidance considers iPadOS devices as having the same use cases and threat scenarios when determining recommendations. In nearly all instances, the configuration steps, default settings, and benchmark recommended settings are identical regardless of hardware platform or operating system. For the few cases where variation exists, the benchmark notes differences within the respective section. 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 support@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 incorporate the Apple iPadOS 18.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. 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://workbench.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, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) '4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - End-User Owned Devices**

  Items in this profile apply to end-user owned Apple iOS 17 and iPadOS 17 devices and intend to:

  - Be practical and prudent.
  - Provide a clear security benefit.
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - End-User Owned Devices**

  This profile extends the "Level 1 - End-User Owned Devices" profile. Items in this profile apply to end-user owned Apple iOS 17 and iPadOS 17 devices and may:

  - Be used for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - Negatively inhibit the utility or performance of the technology.

- **Level 1 - Institutionally-Owned Devices**

  Items in this profile apply to institutionally-owned Apple iOS 17 and iPadOS 17 devices and intend to:

  - Be practical and prudent.
  - Provide a clear security benefit.
  - Not inhibit the utility of the technology beyond acceptable means.

- **Level 2 - Institutionally-Owned Devices**

  This profile extends the "Level 1 - Institutionally-Owned Devices" profile. Items in this profile apply to end-user owned Apple iOS 17 and iPadOS 17 devices and may:

  - Be used for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - 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:

Recommendations

1 Benchmark Guidance

Apple iPadOS provides operating system software to iPad devices. Due to the near identical code base, use cases, threat scenarios, and a shared configuration management mechanism, the CIS Community offers guidance for both operating systems within this single benchmark.

For those unfamiliar with iPadOS device management, a Configuration Profile (CP), which is an XML-formatted file, is the sole natively-supported mechanism for enforcing controls. Whether you're an individual end-user or the administrator for an enterprise deployment, you can create CPs for free using Apple Configurator or with any text editor. Installation of a CP is as simple as connecting a device to the Apple Configurator host via USB, opening the profile on any iOS or iPadOS device, pushing it via macOS Server's Profile Manager, or deploying it via any modern Mobile Device Management (MDM) console.

This benchmark release continues to separate guidance for end-user and institutionally-owned devices. The intention is to scope security control appropriateness by ownership model. This allows the benchmark to address the differing use cases and threat profiles, as well as for an organization to maintain CIS compliance while allowing Bring Your Own Device (BYOD). Look to individual recommendations for specific explanations on the implementation chosen.

In order to support a subset of CP controls, supervision is required to be enabled on all institutionally-owned devices. Supervision is a specific technical state of an iPadOS device. It does not refer to management via CP or MDM console. It can be enabled through Apple's Device Enrollment Program (DEP) in combination with an MDM, or on a per-device basis using Apple Configurator. For more information, see Supervise devices with Apple Configurator 2 for a general overview.

The Additional Recommendations section includes material for both ownership models. Audits, and in some cases remediation, for these recommendations are available with certain MDM solutions.

Thank you for taking the time to read this benchmark guidance.

The CIS iOS and iPadOS Community

2 Configuration Profile Recommendations for End User-Owned Devices

This section provides both level 1 and level 2 recommendations for devices in an unsupervised state. The term "unsupervised" is a specific technical designation regarding the state of an iOS or iPadOS device and does not mean the device is unmanaged. See the introduction of this benchmark for clarification on the states supervised and unsupervised.

The CIS iOS and iPadOS Community further recommends the use of Apple's Volume Purchase Program (VPP) with end user-owned devices. The VPP allows an institution to more effectively manage application licensing by maintaining full ownership and control over applications deployed to end user devices, provided they are managed with an MDM solution.

For more information on the VPP Apple program, visit: [Apple Deployment Programs VPP Guide](#)

2.1 General

2.1.1 (L1) Ensure a "Consent Message" has been "Configured" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the configuration of a consent message shown at the time of a configuration profile installation.

Typically, the enrollment of devices into a Mobile Device Management (MDM) solution requires users to provide their approval. Such approval can waive the need of a consent message. The enrolled MDM must be the organization approved MDM.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the end user. They are voluntarily accepting the configuration profile and should be provided an explicit opportunity to consent.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, verify that under the heading `Consent Message`, there is an appropriate consent message configured.

There is no method to determine if the installed configuration profile included a consent message from the device.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, under the heading `Consent Message`, insert an appropriate consent message.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1** <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1** <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.1.2 (L1) Ensure "Controls when the profile can be removed" is set to "Always" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the removal of a given configuration profile.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the end user. They are voluntarily accepting the configuration profile and should be able to remove it at will.

Impact:

Having a user removing a configuration profile can have impacts for both the organization and the user: the former might lose visibility/control over the device owned by the user, whilst the latter might lose access to the systems due to the removal of the configuration profile.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, verify that under the heading `Security`, the menu `Controls when the profile can be removed` is set to `Always`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Verify `Remove Profile` is displayed near the bottom of the screen.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, under the heading `Security`, set the menu `Controls when the profile can be removed` to `Always`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.2 Restrictions

2.2.1 Functionality

2.2.1.1 (L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to initiating phone calls while a device is locked. Voice dialing is handled separately from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow voice dialing while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Voice dialing while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow voice dialing while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 　　Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> 　　Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.2.1.2 (L1) Ensure "Allow Siri while device is locked" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to accessing Siri while the device is locked.

Rationale:

Accessing Siri on a locked device may allow unauthorized users to access information otherwise not available to them, such as messaging, contacts, and a variety of other data.

Impact:

The end user must unlock the device before interacting with Siri.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow Siri while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Siri while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Siri while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.2.1.3 (L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to managed applications storing and syncing data through iCloud.

Rationale:

This recommendation addresses data leakage. It prevents a user from installing an application that is managed by the organization on a personal device and allowing iCloud to sync the managed application's data to the personal, non-managed application.

Impact:

Syncing managed application data between multiple managed devices will not be possible.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow managed apps to store data in iCloud` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Managed apps cloud sync not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow managed apps to store data in iCloud`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	**13.4 Only Allow Access to Authorized Cloud Storage or Email Providers** Only allow access to authorized cloud storage or email providers.		●	●

2.2.1.4 (L1) Ensure "Force encrypted backups" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to iTunes backup encryption of iOS and iPadOS devices.

Rationale:

Data that are stored securely on an iOS or iPadOS device may be trivially accessed from a local computer backup. Forcing the encryption of backups protects data from being compromised if the local host computer is compromised.

Use of back-ups is strongly advised as they allow to create a copy of data that can be recovered in the event of failures, such as hardware or software failure, data corruption, human-caused event, or accidental deletion of data. Back-up copies allow data to be restored from an earlier point in time to help recovering from an unexpected event.

Impact:

End users must configure a password for the encrypted backup, the complexity of which is not managed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Force encrypted backups` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Encrypted backups enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force encrypted backups`.
5. Deploy the Configuration Profile.

Additional Information:

This function does not apply to iCloud backups. iCloud backups are encrypted in transit and at rest by Apple.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.3 <u>Protect Recovery Data</u> Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	●	●	●
v7	10.4 <u>Ensure Protection of Backups</u> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●

2.2.1.5 (L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

Apple provides a framework that allows advertisers to target Apple users with advertisements relevant to them and their interests by means of a unique identifier. For such personalized advertisements to be delivered, however, detailed information is collected, correlated, and made available to advertisers. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Rationale:

Disabling the use of a unique identifier helps hinder the tracking of users, which in turn supports protection of user data.

Impact:

Users will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow personalized ads delivered by Apple` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Apple personalized advertising not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow personalized ads delivered by Apple`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> 　　Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> 　　Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.1.6 (L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

This recommendation pertains to the acceptance of untrusted TLS certificates.

Rationale:

iOS devices maintain a list of trusted TLS certificate roots. An organization may add their own certificates to the list by using a configuration profile. Allowing users to bypass that list and accept self-signed or otherwise unverified certificates may increase the likelihood of an incident.

Impact:

The device automatically rejects untrusted HTTPS certificates without prompting the user. Services using self-signed certificates will not function.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow users to accept untrusted TLS certificates` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Establishing untrusted TLS connections not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow users to accept untrusted TLS certificates`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 <u>Establish and Maintain a Secure Configuration Process</u>** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 <u>Establish Secure Configurations</u>** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.2.1.7 (L1) Ensure "Force automatic date and time" is set to "Enabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

It is possible to automatically set the date and time on devices running iOS 12 and later. The time zone updates only when the device can determine its location, such as when a device has a cellular connection or a Wi-Fi connection with location services enabled.

Rationale:

Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries.

Impact:

When this option is enabled, users can't turn off `Set Automatically` under `General > Date & Time`

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality` the checkbox for `Force automatic date and time` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Automatic date & time enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force automatic date and time`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4** <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		🟠	🔵
v7	**6.1** <u>Utilize Three Synchronized Time Sources</u> Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		🟠	🔵

2.2.1.8 (L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to Apple's managed application implementation.

The terms "managed" and "unmanaged" refer to application classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned applications are designated as managed. Applications elected by the end user are designated as unmanaged.

Rationale:

Limiting data transfer from the managed institutional application space to the unmanaged user space may prevent data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow documents from managed sources in unmanaged destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from managed to unmanaged apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from managed sources in unmanaged destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3** <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6** <u>Protect Information through Access Control Lists</u> Protect all information stored on systems 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.	●	●	●

2.2.1.9 (L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to Apple's managed application implementation.

The terms "managed" and "unmanaged" refer to application classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned applications are designated as managed. Applications elected by the end user are designated as unmanaged.

Rationale:

Limiting data transfer from the unmanaged user application space to the managed institutional space limits institutional resources from being employed for personal use.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow documents from unmanaged sources in managed destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from unmanaged to managed apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from unmanaged sources in managed destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.2.1.10 (L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to AirDrop in the context of Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to application classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned applications are designated as managed. Applications elected by the end user are designated as unmanaged.

Rationale:

When AirDrop is allowed as a managed destination, sensitive data may be moved out of the managed application space to an unmanaged device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Treat AirDrop as unmanaged destination` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Sharing managed documents using AirDrop not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Treat AirDrop as unmanaged destination`.
5. Deploy the Configuration Profile.

Additional Information:

Note that the feature specifically mentions destination and not source. Following this recommendation does not prevent AirDrop connections into the managed application space, only AirDrop connections out of the managed application space.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.2.1.11 (L2) Ensure "Allow Handoff" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

This recommendation pertains to Apple's Handoff data-sharing mechanism.

Rationale:

Handoff does not enforce managed application boundaries. This allows managed application data to be moved to the unmanaged application space on another device, which may result in data leakage.

Impact:

End users may be inconvenienced by disabling Handoff on their personal devices.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow Handoff` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Handoff not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Handoff`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.2.1.12 (L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

Apple provides a mechanism to send diagnostic and analytics data back to them in order help improve the platform. This information sent to Apple may contain internal organizational information that should not be disclosed to third parties.

Rationale:

Organizations should have knowledge of what is shared with vendors and other third parties, and should also be in full control of what is disclosed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow sending diagnostic and usage data to Apple` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Diagnostic submission not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow sending diagnostic and usage data to Apple`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

2.2.1.13 (L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to configuring wrist detection on paired Apple Watches.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Force Apple Watch wrist detection` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Wrist detection enforced on Apple Watch` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force Apple Watch wrist detection`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.2.1.14 (L1) Ensure "Show Control Center in Lock screen" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the display of Control Center on the lock screen.

Rationale:

When a device is lost or stolen, the Control Center may be used to enable airplane mode, thus preventing locating or erasing the device. Disabling Control Center forces a malicious actor to power down the device, which then discards the encryption key in memory. This makes some attacks based on physical possession more difficult.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Show Control Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Control Center on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Show Control Center in Lock screen`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.2.1.15 (L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the display of Notification Center on the lock screen.

Rationale:

Communications between the operating system and applications to a user should be controlled to prevent data leakage or exploitation. For example, some two-factor authentication applications will present the option to allow a login from a new device in notification center on the lock screen.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Show Notification Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Notifications view on lock screen not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Show Notification Center in Lock screen`.
5. Deploy the Configuration Profile.

Additional Information:

The per-application notification settings described later in the benchmark can be used in lieu of disabling Notification Center at the lock screen. This should only be done if there is confidence that all applications producing sensitive notifications can be managed.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.2.2 Applications

2.2.2.1 (L1) Ensure "Force fraud warning" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the Safari feature which warns end users about visiting suspected fraudulent websites.

Rationale:

Fraudulent websites masquerade as legitimate instances of financial, business, or other sensitive sites. They are designed to capture user credentials, often through phishing campaigns. Safari's fraudulent website warning feature helps protect end users from such sites.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Apps`, the checkbox for `Force fraud warning` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Safari fraud warning enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Apps`, `check` the checkbox for `Force fraud warning`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		●	●
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

2.2.2.2 (L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the automatic acceptance of third-party cookies.

Rationale:

Accepting cookies may allow web servers to interact with other cookies already in place. For example, the HEIST cookie exploit allows for retrieving data from cookies stored on a device. Cookies often follow poor coding practices and include authentication properties. Limiting acceptance of cookies to only those from sites intentionally visited reduces the likelihood of a potential exploit.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Apps`, the menu for `Accept cookies` is set to `From websites I visit` or `From current website only`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Cookie policy enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Apps`, set the `Accept cookies` menu to `From websites I visit` or `From current website only`.
5. Deploy the Configuration Profile.

Additional Information:

`From websites I visit` accepts cookies from the current domain and any domain you've visited. `From current website only` only accepts cookies from the current domain.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.4 <u>Restrict Unnecessary or Unauthorized Browser and Email Client Extensions</u> Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.		🟠	🔵
v7	7.2 <u>Disable Unnecessary or Unauthorized Browser or Email Client Plugins</u> Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		🟠	🔵

2.3 Domains

2.3.1 (L1) Ensure "Managed Safari Web Domains" is "Configured" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to whether Safari, as well as Mobile Device Management (MDM) deployed browsers, will consider certain URL patterns for managed application spaces only.

Rationale:

Sensitive files available from a website may be downloaded into the unmanaged application spaces by default. By configuring specific domains that Safari should consider managed, an institution may support the secure containerization of their data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Domains` tab.
4. In the right window pane, verify that under `Managed Safari Web Domains` each appropriate URL pattern is configured.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Domains` tab.
4. In the right window pane, under `Managed Safari Web Domains` enter the appropriate URL pattern(s).
5. Deploy the Configuration Profile.

Additional Information:

For improved effectiveness, this recommendation should be paired with the blacklisting of web browsers not deployed through the MDM.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.4 Passcode

2.4.1 (L1) Ensure "Allow simple value" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to passcode requirements. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA).

Rationale:

Simple passcodes include repeating, ascending, or descending character sequences that may be easily guessed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the checkbox for `Allow simple value` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Simple passcodes allowed` displays `No`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, `uncheck` the checkbox for `Allow simple value`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.4.2 (L2) Ensure "Require alphanumeric value" is set to "Enabled" (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

Passwords set by users must contain at least one letter and one number.

Rationale:

Complex passwords are more resistant against persons seeking unauthorized access to a system.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the checkbox for `Require alphanumeric value` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Require alphanumeric value` displays `Yes`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, `check` the checkbox for `Require alphanumeric value`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.4.3 (L1) Ensure "Minimum passcode length" is set to a value of "6" or greater (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to minimum passcode length.

Rationale:

Requiring at least six character minimum length provides reasonable assurance against passcode attacks.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the `Minimum passcode length` is set to `6`, or greater.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Minimum length` displays `6`, or greater.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Minimum passcode length` to `6`, or greater.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 　Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> 　Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.4.4 (L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the maximum number of minutes a device may remain inactive before auto-locking.

Note: This recommendation refers to maximum auto-lock, consistent with the interface language, but iOS and iPadOS devices treat the auto-lock function as equaling exactly 2 minutes.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a passcode.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the `Maximum Auto-Lock` is set to `2 minutes`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max inactivity` displays `2 minutes`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum Auto-Lock` to `2 minutes`.
5. Deploy the Configuration Profile.

Additional Information:

This is not enforced during certain activities; such as watching movies.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.4.5 (L1) Ensure "Maximum grace period for device lock" is set to "Immediately" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the amount of time a device may be unlocked without entering a passcode after that device has been locked. Devices with TouchID enabled do not allow a grace period.

Rationale:

Configuring the `Maximum grace period for device lock` to `Immediately` precludes unauthenticated access when waking the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that `Maximum grace period for device lock` is set to `Immediately`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max grace period` displays `Immediately`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum grace period for device lock` to `Immediately`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.4.6 (L1) Ensure "Maximum number of failed attempts" is set to "6" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the number of attempted logins before automatic deletion of a device's cryptographic key.

Rationale:

Excessive incorrect passcode attempts typically indicate that the owner has lost physical control of the device. In the event of such an incident, erasing the encryption key will help to ensure confidentiality of information stored on the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that `Maximum number of failed attempts` is set to `6`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max failed attempts` displays `6`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum number of failed attempts` to `6`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u>** Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	**5.1 <u>Establish Secure Configurations</u>** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.5 Wi-Fi

2.5.1 (L1) Ensure "Disable Association MAC Randomization" is "Configured" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to disabling MAC randomization as needed. MAC addresses can still be used as part of inventory management and may be desired on internal networks. User privacy concerns should recommend allowing the setting on other networks.

Rationale:

MAC randomization is a feature available from iOS 14 onward and is enabled by default. Although this feature enhances privacy for individuals by using random and different addresses for each Wi-Fi network, it can lead to problems in some circumstances, such as captive portals, MAC-based Access Control Lists, etc. In such cases, disabling this feature may be necessary. This is a per-network setting, meaning it can be turned off for specific networks only.

Audit:

This is a per-network configuration setting, the auditor will need to determine which solution is appropriate for a specific network.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Wi-Fi` tab.
4. In the right window pane, select the relevant Wi-Fi configuration.
5. Verify that the checkbox for `Disable Association MAC Randomization` is `checked`.

From the device:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Tap the relevant network.
4. Ensure `Private Address` is `disabled`.

Remediation:

This remediation procedure cannot be accomplished with a checkbox, it needs to be applied on a per-network basis as appropriate.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Wi-Fi` tab.
4. In the right window pane, select the relevant Wi-Fi configuration.
5. In the right window pane, check the checkbox for `Disable Association MAC Randomization`.
6. Deploy the Configuration Profile.

From the device:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Tap the relevant network.
4. Disable the option `Private Address`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.6 VPN

2.6.1 (L1) Ensure "VPN" is "Configured" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to establishing a virtual private network (VPN) connection when appropriate.

Rationale:

The network to which a device connects provides important services that may be exploited by a malicious actor. Establishing a VPN mitigates the associated risks by encrypting data in transit and using known good network services, such as DNS.

Audit:

This audit procedure cannot be accomplished with a checkbox verification. As mentioned below, a per-application VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. The auditor will need to determine which solution, and to what extent in the per-application VPN case, is appropriate.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the VPN tab.
4. In the right window pane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device:

1. Tap Settings.
2. Tap General.
3. Tap VPN.
4. Inspect the configuration.

Remediation:

This remediation procedure cannot be accomplished with a checkbox. As mentioned below, a per-application VPN configuration is the preferred option, but a system-wide VPN is also acceptable. An appropriate solution will need to be determined and implemented.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the VPN tab.
4. In the right window pane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Enter an appropriate VPN configuration.

References:

1. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW37

Additional Information:

iOS and iPadOS support both per-application VPN and system-wide VPN. Per-application configuration is preferred because it is always on, managed entirely through the configuration profile and/or Mobile Device Management (MDM), and invisible to the end-user.

CIS Benchmarks do not recommend specific VPN settings, as these depend on each organization capability, however it strongly suggests industry or governmental guidance to be followed.

References:

- https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
- https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf
- https://support.apple.com/en-ca/guide/deployment-reference-ios/ior9f7b5ff26/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●

2.7 Mail

2.7.1 (L1) Ensure "Allow user to move messages from this account" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to whether a message can be moved from an institutionally-configured mail account to an end user-configured mail account. It also limits forwarding or replying from a different account than the one from which the message originated.

Note: This recommendation only applies if an institutionally-configured mail account resides on the device.

Rationale:

Allowing the movement of messages from a managed email account to an unmanaged email account may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, verify that the checkbox for `Allow user to move messages from this account` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, check the checkbox for `Allow user to move messages from this account`.

Default Value:

Message movement, forwarding, and replying are unrestricted.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.7.2 (L1) Ensure "Allow Mail Drop" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to whether a message attachment can be uploaded or accessed through Apple's Mail Drop service. This is a system-wide setting and would block Mail Drop for any personal accounts on the device using Apple Mail.

This recommendation does not need to be configured if your organization is using an email application other than Apple Mail.

Rationale:

Permitting attachment uploads to Mail Drop, which is outside organizational control, presents a data exfiltration path.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, verify that the checkbox for `Allow Mail Drop` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, uncheck the checkbox for `Allow Mail Drop`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

2.8 Notifications

2.8.1 (L1) Ensure "Notification Settings" are configured for all "Managed Apps" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to the configuration of notification settings on a per-application basis.

Rationale:

Notifications may include sensitive data or might allow for privileged actions to take place. All managed applications must include explicit notification settings in order to address these concerns.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Notifications` tab.
4. In the right window pane, verify that each managed app includes a configuration entry.

Or, from the device:

1. Tap `Settings`.
2. Tap `Notifications`.
3. Verify that managed apps are grayed out to indicate that their notification settings are managed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Notifications` tab.
4. In the right window pane, click `Configure` and/or click the + to add notification settings on a per-app basis.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3 Configuration Profile Recommendations for Institutionally-Owned Devices

This section provides both level 1 and level 2 recommendations for devices in a supervised state. The term "supervised" is a specific technical designation in regards to the state of an iOS or iPadOS device and is generally only applied to institutionally-owned devices. See the introduction of this benchmark for clarification on the states supervised and unsupervised.

The CIS iOS and iPadOS Community further recommends the use of Apple's Device Enrollment Program (DEP) and Volume Purchase Program (VPP) with institutionally-owned devices. The DEP associates devices owned by an institution with its MDM server(s). The association occurs during setup when the iOS or iPadOS device contacts an Apple activation server. This ensures that all devices owned by an institution are being managed by its MDM solution, and allows for the distribution of iOS or iPadOS devices brand new or restored to factory default because they will receive configuration at activation. The VPP allows an institution to more effectively manage app licensing by maintaining full ownership and control over apps deployed within the organization. This can be especially useful for shared devices where managing AppleID app ownership is impractical.

For more information on these two Apple programs, visit: https://www.apple.com/business/enterprise/it/

3.1 General

3.1.1 (L1) Ensure "Controls when the profile can be removed" is set to "Never" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the removal of a given configuration profile.

Typically, the enrollment of devices into a Mobile Device Management (MDM) does not allow a user to remove any managed configurations.

Rationale:

In this section of the benchmark, recommendations are for devices that are owned by the institution. Removal of the configuration profile should be at the discretion of the institution, not the end user, in order to prevent weakening the device's security and exposing its data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, verify that under the heading `Security`, the menu `Controls when the profile can be removed` is set to `Never`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Verify `Remove Profile` is **not** displayed near the bottom of the screen.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `General` tab.
4. In the right window pane, under the heading `Security`, set the menu `Controls when the profile can be removed` to `Never`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1** <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1** <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2 Restrictions

3.2.1 Functionality

3.2.1.1 (L2) Ensure "Allow screenshots and screen recording" is set to "Disabled" (Manual)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to limiting screenshots and screen recordings.

Rationale:

Sensitive information may be displayed through a managed application that could be captured by screenshot or screen recording into the unmanaged space inadvertently or intentionally by a malicious insider.

Impact:

Screenshots will be unavailable for troubleshooting.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow screenshots and screen recording` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Screen capture and recording not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow screenshots and screen recording`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.2.1.2 (L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to initiating phone calls while a device is locked. Voice dialing is handled separately from Siri.

Rationale:

Allowing calls from a locked device may allow for the impersonation of the device owner.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow voice dialing while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Voice dialing while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow voice dialing while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.2.1.3 (L1) Ensure "Allow Siri while device is locked" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to access to Siri while the device is locked.

Rationale:

Accessing Siri on a locked device may allow unauthorized users to access information otherwise not available to them, such as messaging, contacts, and a variety of other data.

Impact:

The end user must unlock the device before interacting with Siri.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow Siri while device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Siri while locked not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Siri while device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.2.1.4 (L1) Ensure "Allow iCloud backup" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to allowing iCloud backup.

This recommendation does block educational institutions from being able to use iCloud backup with devices issued to students. Because of this, we do not recommend educational institutions enable this recommendation for those devices.

Rationale:

iCloud backups are encrypted in transit and at rest within Apple's infrastructure, but there is no protection against restoring a backup to an unmanaged device. This potentially allows for data leakage.

Use of back-ups is strongly advised as they allow to create a copy of data that can be recovered in the event of failures, such as hardware or software failure, data corruption, or a human-caused event, or accidental deletion of data. Back-up copies allow data to be restored from an earlier point in time to help recovering from an unexpected event.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud backup` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud backup not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud backup`.
5. Deploy the Configuration Profile.

Additional Information:

This recommendation is exclusively for institutionally-owned devices. If an institution is relying on Bring Your Own Device (BYOD), those devices should not contain sensitive material necessary to protect at this level.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	**13.4 Only Allow Access to Authorized Cloud Storage or Email Providers** Only allow access to authorized cloud storage or email providers.		●	●

3.2.1.5 (L1) Ensure "Allow iCloud documents & data" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the storage and syncing of data through iCloud from institutionally-owned devices.

Rationale:

Institutionally-owned devices are often connected to personal iCloud accounts. This is expected and normal. The data from institutionally-owned devices, however, should not co-mingle with the end-user's personal data. This creates a potential avenue for data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow iCloud documents & data` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Documents in the Cloud not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud documents & data`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	🟢	🟠	🔵
v7	**13.4 Only Allow Access to Authorized Cloud Storage or Email Providers** Only allow access to authorized cloud storage or email providers.		🟠	🔵

3.2.1.6 (L1) Review "Allow iCloud Keychain" settings (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

iCloud Keychain allows passwords associated with an Apple Account to be used by the authenticated user for their Apple Account. If an organization's users are using personal Apple Accounts with organization owned devices, than organizations should review whether enterprise passwords/passkeys/accounts are being stored in users' personal iCloud Keychain. To review the possibility of those enterprise credentials being stored, you can start by using your organization's MDM platform to verify which users are signed into their personal Apple Accounts and have iCloud Keychain syncing enabled.

Note: In previous versions of the benchmark, we stated that iCloud Keychain was unencrypted. Apple has upgraded the encryption on iCloud Keychain to include end-to-end encryption under both the standard and advanced data protection options. To view more about iCloud encryption, plus the differences between the standard data protection and advanced data protection, you can read Apple's support article iCloud data security overview.

Rationale:

It is normal and expected for end users to configure their personal iCloud account on an institutionally-owned device. Because of this, disabling iCloud Keychain prevents OS-automated credential transfer to devices outside organizational control, thus reducing the risk for misuse of those credentials from unauthorized devices.

Impact:

Several risk aspects should be reviewed prior to disabling iCloud Keychain:

- At this point, iCloud Keychain only stores passwords. Where Multi-Factor Authentication, Single-Sign-On, or device-based profiles are used, those credentials will not make use of iCloud Keychain synchronization. Mature enterprises should no longer be solely using password authentication, and thus should not be at risk through the use of iCloud Keychain.
- iCloud Keychain synchronizes user passwords. A user presumably already knows these passwords and periodically changes them. They might also use passwords from an unauthorized device without iCloud synchronization. Ideally the institutionally-issued device has greater access than an unauthorized or public device to the authentication server. If the personal device cannot logically engage with the authentication service, then the risk of password synchronization is also greatly reduced.
- Blocking the use of iCloud Keychain also blocks synchronization of non-enterprise-managed accounts that the user may need for their regular work. This also blocks the use of strong, unique password suggestions made available by Apple.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow iCloud Keychain` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `iCloud Keychain not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow iCloud Keychain`.
5. Deploy the Configuration Profile.

References:

1. https://support.apple.com/en-us/102651

Additional Information:

This recommendation is not intended as advice against using the Keychain locally on an institutionally-owned device, nor is it intended to be taken as a recommendation to prevent iCloud Keychain from being used on end user-owned devices.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v8	15.3 Classify Service Providers Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.2.1.7 (L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to managed applications storing and syncing data through iCloud.

Rationale:

This recommendation addresses data leakage. It prevents a user from installing an application that is managed by the organization on a personal device and allowing iCloud to sync the managed application's data to the personal, non-managed application.

Impact:

Data created on the device may be lost if the end user has not transferred it to another device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow managed apps to store data in iCloud` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Managed apps cloud sync not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow managed apps to store data in iCloud`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	**13.4 Only Allow Access to Authorized Cloud Storage or Email Providers** Only allow access to authorized cloud storage or email providers.		●	●

3.2.1.8 (L2) Ensure "Allow USB drive access in Files app" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to preventing the Files app from accessing USB media.

Rationale:

The Files app provides a local file system and interface to USB media for iOS and iPadOS devices. In environments with sensitive data and strict data loss prevention policies, disabling the use of USB media with such devices may reduce the risk of data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow USB drive access in Files app` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `USB drives not accessible in Files app` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow USB drive access in Files app`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**1.2 Address Unauthorized Assets** Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	●	●	●
v7	**13.7 Manage USB Devices** If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

3.2.1.9 (L2) Ensure "Allow network drive access in Files app" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to preventing the Files app from accessing networking file shares.

Rationale:

The Files app provides a local file system and interface to network file shares for iOS and iPadOS devices. In environments with sensitive data and strict data loss prevention policies, disabling the use of network file shares with such devices may reduce the risk of data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow network drive access in Files app` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Network drives not accessible in Files app` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow network drive access in Files app`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 Address Unauthorized Assets Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	●	●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

3.2.1.10 (L1) Ensure "Force encrypted backups" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to iTunes backup encryption of iOS and iPadOS devices.

Rationale:

Data that are stored securely on an iOS or iPadOS device may be trivially accessed from a local computer. Forcing the encryption of backups significantly reduces the likelihood of sensitive data being compromised if the local host computer is compromised.

Impact:

End users must configure a password for the encrypted backup, the complexity of which is not managed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Force encrypted backups` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Encrypted backups enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force encrypted backups`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**11.3 Protect Recovery Data** Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	●	●	●
v7	**10.4 Ensure Protection of Backups** Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●

3.2.1.11 (L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

Apple provides a framework that allows advertisers to target Apple users with advertisements relevant to them and their interests by means of a unique identifier. For such personalized advertisements to be delivered, however, detailed information is collected, correlated, and made available to advertisers. This information is valuable to both advertisers and attackers and has been used with other metadata to reveal users' identities.

Rationale:

Disabling the use of a unique identifier helps hinder the tracking of users, which in turn supports protection of user data.

Impact:

Users will see generic advertising rather than targeted advertising. Apple warns that this will reduce the number of relevant ads.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow personalized ads delivered by Apple` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Apple personalized advertising not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow personalized ads delivered by Apple`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	🟢	🟠	🔵
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	🟢	🟠	🔵
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

3.2.1.12 (L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the factory reset functionality of iOS and iPadOS devices.

Rationale:

An institutionally-owned device should not allow an end user to destroy data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow Erase All Content and Settings` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Erase content and settings not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Erase All Content and Settings`.
5. Deploy the Configuration Profile.

Additional Information:

An end-user may still employ Apple's Find My iPhone/iPad service to perform an Erase All Content and Settings. This also sets an activation lock on the device. Activation lock may be blocked using a Mobile Device Management (MDM) solution, but not via configuration profile.

For more information, see https://support.apple.com/en-us/HT202804

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.1.13 (L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to the acceptance of untrusted TLS certificates.

Rationale:

iOS devices maintain a list of trusted TLS certificate roots. An organization may add their own certificates to the list by using a configuration profile. Allowing users to bypass that list and accept self-signed or otherwise unverified certificates may increase the likelihood of an incident.

Impact:

The device automatically rejects untrusted HTTPS certificates without prompting the user.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow users to accept untrusted TLS certificates` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Establishing untrusted TLS connections not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow users to accept untrusted TLS certificates`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.1.14 (L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to permitting application installation by end users from outside the Apple App Store or Mobile Device Management (MDM) deployment.

Rationale:

Allowing application installation by end users from outside of the Apple App Store or Mobile Device Management (MDM) may permit a user to install a malicious application.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow trusting new enterprise app authors` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Allow trusting new enterprise app authors not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow trusting new enterprise app authors`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.3 Address Unauthorized Software** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	**2.6 Address unapproved software** Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

3.2.1.15 (L1) Ensure "Allow installing configuration profiles" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the installation of additional configuration profiles.

Rationale:

This recommendation allows an institution to ensure that only the configuration profiles they provide are loaded onto the device.

Impact:

Some services, such as WiFi hotspot networks, may be prevented from working by blocking their configuration profiles.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow installing configuration profiles` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Installing configuration profiles not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow installing configuration profiles`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 <u>Establish and Maintain a Secure Configuration Process</u>** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 <u>Establish Secure Configurations</u>** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.1.16 (L1) Ensure "Allow adding VPN configurations" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the addition of user-defined VPN configurations.

Rationale:

This recommendation allows an institution to ensure that only the VPN configurations they provide are loaded onto the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow adding VPN configurations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `VPN creation not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow adding VPN configurations`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure** Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.2.1.17 (L1) Ensure "Force automatic date and time" is set to "Enabled" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

It is possible to automatically set the date and time on devices running iOS 12 and later. The time zone updates only when the device can determine its location, such as when a device has a cellular connection or a Wi-Fi connection with location services enabled.

Rationale:

Correct date and time settings are required for authentication protocols, file creation, modification dates, and log entries.

Impact:

When this option is enabled, users can't turn off `Set Automatically` under `General` > `Date & Time`

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality` the checkbox for `Force automatic date and time` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Automatic date & time enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force automatic date and time`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.4 Standardize Time Synchronization** Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		🟠	🔵
v7	**6.1 Utilize Three Synchronized Time Sources** Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		🟠	🔵

3.2.1.18 (L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to modifying the use of cellular data by applications.

Rationale:

It is appropriate for an institution to have remote locating and erasure capability with their devices. Forcing cellular data to remain active supports that functionality.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow modifying cellular data app settings` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Changing app cellular data usage not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow modifying cellular data app settings`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.1.19 (L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to allowing USB devices communicate with a locked device.

Rationale:

Physical attacks against iOS and iPadOS devices have been developed that exploit the trust of physically-connected accessories. This has led to proof-of-concept data extraction and even commercially available hardware designed to perform such attacks. By requiring the device to be unlocked in order to remove data, this control reduces the probability of a successful data extraction.

Impact:

An end user will not be able to connect their device to a USB accessory while the device is locked.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow USB accessories while the device is locked` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `USB accessories while locked allowed` is **NOT** displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow USB accessories while the device is locked`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.2 <u>Address Unauthorized Assets</u> Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	●	●	●
v7	13.7 <u>Manage USB Devices</u> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

3.2.1.20 (L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled" (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to allowing data communication with a host computer.

Rationale:

Host pairing is a process by which an iOS or iPadOS device creates a cryptographically verified connection with a trusted host computer. By disabling the addition of new host pairings, a variety of hardware-based attacks on the device are blocked.

Impact:

An end user will not be able to sync media to and from the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow pairing with non-Configurator hosts` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Pairing with iTunes not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow pairing with non-Configurator hosts`.
5. Deploy the Configuration Profile.

Additional Information:

There are two important pieces of data on the Apple Configurator host. The login keychain will include the host's identity certificate and may be exported. The escrow keybags related to each device will be found in /var/db/lockdown. It is important that both these be backed up for continuity of device management. They may also be duplicated to other Macs to allow management of the configured devices.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	**15.6 Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients** Disable peer-to-peer (adhoc) wireless network capabilities on wireless clients.		🟠	🔵

3.2.1.21 (L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to Apple's managed application implementation.

The terms "managed" and "unmanaged" refer to app classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned apps are designated managed. Apps elected by the end user are designated unmanaged.

Rationale:

Limiting data transfer from the managed institutional application space to the user space may prevent data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow documents from managed sources in unmanaged destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from managed to unmanaged apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from managed sources in unmanaged destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.2.1.22 (L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to Apple's managed application implementation.

The terms "managed" and "unmanaged" refer to application classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned applications are designated as managed. Applications elected by the end user are designated as unmanaged.

Rationale:

Limiting data transfer from the unmanaged user application space to the managed institutional space limits institutional resources from being employed for personal use.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow documents from unmanaged sources in managed destinations` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Opening documents from unmanaged to managed apps not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow documents from unmanaged sources in managed destinations`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3** <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6** <u>Protect Information through Access Control Lists</u> Protect all information stored on systems 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.	●	●	●

3.2.1.23 (L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to AirDrop in the context of Apple's managed app implementation.

The terms "managed" and "unmanaged" refer to application classifications made through Managed Open In, a feature introduced in iOS 7. Managed Open In provides for data containerization. Institutionally-provisioned applications are designated as managed. Applications elected by the end user are designated as unmanaged.

Rationale:

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Treat AirDrop as unmanaged destination` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Sharing managed documents using AirDrop not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Treat AirDrop as unmanaged destination`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**6.7 Centralize Access Control** Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	**4.8 Log and Alert on Changes to Administrative Group Membership** Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	**15.4 Disable Wireless Access on Devices if Not Required** Disable wireless access on devices that do not have a business purpose for wireless access.			●

3.2.1.24 (L1) Ensure "Allow Handoff" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to Apple's Handoff data-sharing mechanism.

Rationale:

Handoff does not enforce managed application boundaries. This allows managed application data to be moved to the unmanaged application space on another device, which may result in data leakage.

Impact:

End users may be inconvenienced by disabling Handoff on their personal devices.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow Handoff` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Handoff not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow Handoff`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.2.1.25 (L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

Apple provides a mechanism to send diagnostic and analytics data back to them in order help improve the platform. This information sent to Apple may contain internal organizational information that should not be disclosed to third parties.

Rationale:

Organizations should have knowledge of what is shared with vendors and other third parties, and should also be in full control of what is disclosed.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow sending diagnostic and usage data to Apple` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Diagnostic submission not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow sending diagnostic and usage data to Apple`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.2.1.26 (L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to forcing re-authentication at each AutoFill operation.

Rationale:

A device may be accessed by an unauthorized user while unlocked. This recommendation provides defense-in-depth by forcing re-authentication before credentials will be populated by AutoFill.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Require Touch ID / Face ID authentication before AutoFill` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Authentication before Auto Filling passwords enforced` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Require Touch ID / Face ID authentication before AutoFill`.
5. Deploy the Configuration Profile.

Additional Information:

The benchmark remains intentionally silent on permitting the use of the local Apple Keychain, deferring to each institution to consider its own circumstances and associated risk.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.2.1.27 (L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to configuring wrist detection on paired Apple Watches.

Rationale:

Wrist detection prevents a removed Apple Watch from providing access to information not otherwise available.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Force Apple Watch wrist detection` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Wrist detection enforced on Apple Watch` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `check` the checkbox for `Force Apple Watch wrist detection`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.2.1.28 (L1) Ensure "Allow setting up new nearby devices" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to Apple's *Quick Start* setup feature.

Rationale:

This recommendation prevents an institutionally-owned device from transferring configurations or content to another device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow setting up new nearby devices` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Proximity Setup to a new device is not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow setting up new nearby devices`.
5. Deploy the Configuration Profile.

Additional Information:

For more information on *Quick Start*, see: https://support.apple.com/en-us/HT201269

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.13** <u>Deploy a Data Loss Prevention Solution</u> Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	**13.3** <u>Monitor and Block Unauthorized Network Traffic</u> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

3.2.1.29 (L1) Ensure "Allow proximity based password sharing requests" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to preventing proximity-based password sharing from institutionally-owned devices.

Rationale:

In an organizational context, access to systems and applications should be provisioned by role, with credentials only being transferred through supported credential management systems. Additionally, credential sharing requests may be exploited through a social engineering scheme.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow proximity based password sharing requests` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Proximity password requests not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow proximity based password sharing requests`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**13.5** <u>Manage Access Control for Remote Assets</u> Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v7	**12.12** <u>Manage All Devices Remotely Logging into Internal Network</u> Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			●

3.2.1.30 (L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to sharing credentials between devices, such as through AirDrop.

Rationale:

Allowing password sharing may increase the likelihood of an institutionally related credential being moved to a non-institutionally controlled device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Allow password sharing (supervised only)` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Restrictions`.
7. Confirm `Password sharing is not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow password sharing (supervised only)`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**13.5 Manage Access Control for Remote Assets** Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		🟠	🔵
v8	**14.3 Train Workforce Members on Authentication Best Practices** Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	🟢	🟠	🔵
v7	**12.12 Manage All Devices Remotely Logging into Internal Network** Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			🔵
v7	**17.5 Train Workforce on Secure Authentication** Train workforce members on the importance of enabling and utilizing secure authentication.	🟢	🟠	🔵

3.2.1.31 (L1) Ensure "Show Control Center in Lock screen" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the display of Control Center on the lock screen.

Rationale:

When a device is lost or stolen, the Control Center may be used to enable airplane mode, thus preventing locating or erasing the device. It forces a malicious actor to power down the device, which then discards the encryption key in memory. This makes other attacks based on physical possession more difficult.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Show Control Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Control Center view on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Show Control Center in Lock screen`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.2.1.32 (L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the display of Notification Center on the lock screen.

Rationale:

Communications between the operating system and applications to a user should be controlled to prevent data leakage or exploitation. For example, some two-factor authentication applications will present the option to allow a login from a new device in notification center on the lock screen.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, the checkbox for `Show Notification Center in Lock screen` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Notifications view on lock screen not allowed` is displayed

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Show Notification Center in Lock screen`.
5. Deploy the Configuration Profile.

Additional Information:

The per-application notification settings described later in the benchmark can be used in lieu of disabling Notification Center at the lock screen. This should only be done if there is confidence that all applications producing sensitive notifications can be managed.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.2.2 Apps

3.2.2.1 (L1) Ensure "Force fraud warning" is set to "Enabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the Safari feature which warns end users about visiting suspected fraudulent websites.

Rationale:

Enabling a warning may help users avoid accidentally visiting known phishing or other fraudulent sites covered by this feature.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Apps`, the checkbox for `Force fraud warning` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Safari fraud warning enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Apps`, `check` the checkbox for `Force fraud warning`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.2.2 (L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the acceptance of third-party cookies.

Rationale:

The HEIST cookie exploit allows for retrieving data from cookies stored on a device. Cookies often follow poor coding practices and often include authentication properties. Limiting acceptance of cookies to only those from sites intentionally visited reduces the likelihood of exploitation.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Apps`, the menu for `Accept cookies` is set to `From websites I visit` or `From current website only`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `Cookie policy enforced` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Apps`, set the `Accept cookies` menu to `From websites I visit` or `From current website only`.
5. Deploy the Configuration Profile.

Additional Information:

`From websites I visit` accepts cookies from the current domain and any other domain you've visited. `From current website only` only accepts cookies from the current domain.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.3 Domains

3.3.1 (L1) Ensure "Managed Safari Web Domains" is "Configured" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to whether Safari, as well as Mobile Device Management (MDM) deployed browsers, will consider certain URL patterns for managed application spaces only.

Rationale:

Sensitive files available from a website may be downloaded into the unmanaged application spaces by default. By configuring specific domains that Safari should consider managed, an institution may support the secure containerization of their data.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, verify that under `Managed Safari Web Domains` each appropriate URL pattern is configured.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Domains` tab.
4. In the right windowpane, under `Managed Safari Web Domains` enter the appropriate URL pattern(s).
5. Deploy the Configuration Profile.

Additional Information:

For improved effectiveness, this recommendation should be paired with the blacklisting of web browsers not deployed through the MDM.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.4 Passcode

3.4.1 (L1) Ensure "Allow simple value" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to passcode requirements. A simple passcode is defined as containing repeated characters, or increasing/decreasing characters (such as 123 or CBA).

Rationale:

Simple passcodes such as those with repeating, ascending, or descending character sequences are easily guessed. Preventing the selection of passwords containing such sequences increases the complexity of the passcode and reduces the ease with which an attacker may attempt to guess the passcode in order to gain access to the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the checkbox for `Allow simple value` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Simple passcodes allowed` displays `No`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, `uncheck` the checkbox for `Allow simple value`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

3.4.2 (L2) Ensure "Require alphanumeric value" is set to "Enabled" (Manual)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

Passwords set by users must contain at least one letter and one number.

Rationale:

Complex passwords are more resistant against persons seeking unauthorized access to a system.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the checkbox for `Require alphanumeric value` is `checked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Require alphanumeric value` displays `Yes`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, `check` the checkbox for `Require alphanumeric value`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4** <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

3.4.3 (L1) Ensure "Minimum passcode length" is set to a value of "6" or greater (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to minimum passcode length.

Rationale:

Requiring at least six character minimum length provides reasonable assurance against passcode attacks.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the `Minimum passcode length` is set to `6`, or greater.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Minimum length` displays `6`, or greater.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Minimum passcode length` to `6`, or greater.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	**4.4** <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

3.4.4 (L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the maximum number of minutes a device may remain inactive before auto-locking.

Note: This recommendation refers to maximum auto-lock, consistent with the interface language, but iOS and iPadOS devices treat the auto-lock function as equaling exactly 2 minutes.

Rationale:

Automatically locking the device after a short period of inactivity reduces the probability of an attacker accessing the device without entering a password.

Impact:

This is not enforced during certain activities, such as watching movies.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that the `Maximum Auto-Lock` is set to `2 minutes`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max inactivity` displays `2 minutes`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum Auto-Lock` to `2`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.4.5 (L1) Ensure "Maximum grace period for device lock" is set to "Immediately" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the amount of time a device may be unlocked without entering a passcode after that device has been locked. Devices with TouchID enabled do not allow a grace period.

Rationale:

Configuring the `Maximum grace period for device lock` to `Immediately` precludes unauthenticated access when waking the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that `Maximum grace period for device lock` is set to `Immediately`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max grace period` displays `Immediately`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum grace period for device lock` to `Immediately`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.4.6 (L1) Ensure "Maximum number of failed attempts" is set to "6" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the number of attempted logins before automatic deletion of a device's cryptographic key.

Rationale:

Excessive incorrect passcode attempts typically indicate that the owner has lost physical control of the device. In the event of such an incident, erasing the encryption key will help to ensure confidentiality of information stored on the device.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, verify that `Maximum number of failed attempts` is set to `6`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Tap `Passcode`.
7. Confirm `Max failed attempts` is set to `6`.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Passcode` tab.
4. In the right window pane, set the `Maximum number of failed attempts` to `6`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

3.5 Wi-Fi

3.5.1 (L1) Ensure "Disable Association MAC Randomization" is "Configured" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to disabling MAC randomization as needed.

Rationale:

MAC randomization is a feature available from iOS 14 onward and is enabled by default. Although this feature enhances privacy for individuals by using random and different addresses for each Wi-Fi network, it can lead to problems in some circumstances, such as captive portals, MAC-based Access Control Lists, etc. In such cases, disabling this feature may be necessary. This is a per-network setting, meaning it can be turned off for specific networks only.

Audit:

This is a per-network configuration setting, the auditor will need to determine which solution is appropriate for a specific network.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Wi-Fi` tab.
4. In the right window pane, select the relevant Wi-Fi configuration.
5. Verify that the checkbox for `Disable Association MAC Randomization` is `checked`.

From the device:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Tap the relevant network.
4. Ensure `Private Address` is `disabled`.

Remediation:

This remediation procedure cannot be accomplished with a checkbox, it needs to be applied on a per-network basis as appropriate.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Wi-Fi` tab.
4. In the right window pane, select the relevant Wi-Fi configuration.
5. In the right window pane, check the checkbox for `Disable Association MAC Randomization`.
6. Deploy the Configuration Profile.

From the device:

1. Tap `Settings`.
2. Tap `Wi-Fi`.
3. Tap the relevant network.
4. Disable the option `Private Address`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.6 VPN

3.6.1 (L1) Ensure "VPN" is "Configured" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to establishing a virtual private network (VPN) connection as needed.

Rationale:

The network to which a device connects provides important services that may be exploited by a malicious actor. Establishing a VPN mitigates the associated risks by encrypting data in transit and using known good network services, such as DNS.

Audit:

This audit procedure cannot be accomplished with a checkbox verification. As mentioned below, a per-application VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. The auditor will need to determine which solution is appropriate, and to what extent on a per-application VPN case.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the VPN tab.
4. In the right window pane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN`.
4. Inspect the configuration.

Remediation:

This remediation procedure cannot be accomplished with a checkbox. As mentioned below, a per-application VPN configuration is the preferred solution, but a system-wide VPN is also acceptable. An appropriate solution will need to be determined and implemented.
From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the VPN tab.
4. In the right window pane, enter an appropriate VPN configuration.
5. Deploy the Configuration Profile.

From the device,

1. Tap Settings.
2. Tap General.
3. Tap VPN.
4. Enter an appropriate VPN configuration.

References:

1. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW37
2. https://developer.apple.com/library/content/featuredarticles/iPhoneConfigurationProfileRef/Introduction/Introduction.html#//apple_ref/doc/uid/TP40010206-CH1-SW27

Additional Information:

iOS 11 supports both per-application VPN and system-wide VPN. Per-application configuration is preferred because it is always on, managed entirely through the configuration profile and/or Mobile Device Management (MDM), and invisible to the end-user.

CIS Benchmarks do not recommend specific VPN settings, as these depend on each organization capability, however it strongly suggests industry or governmental guidance to be followed.

References:

- https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
- https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf
- https://support.apple.com/en-ca/guide/deployment-reference-ios/ior9f7b5ff26/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

3.7 Mail

3.7.1 (L1) Ensure "Allow user to move messages from this account" is set to "Disabled" (Automated)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to whether a message can be moved from an institutionally-configured mail account to an end user-configured mail account. It also limits forwarding or replying from a different account than the one from which the message originated.

Note: This recommendation only applies if an institutionally-configured mail account resides on the device.

Rationale:

Allowing the movement of messages from a managed email account to an unmanaged email account may result in data leakage.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, verify that the checkbox for `Allow user to move messages from this account` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Mail` tab.
4. In the right window pane, uncheck the checkbox for `Allow user to move messages from this account`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 Configure Data Access Control Lists** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 Protect Information through Access Control Lists** Protect all information stored on systems 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.	●	●	●

3.7.2 (L2) Ensure 'Allow Mail Drop' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to whether a message attachment can be uploaded and accessed through Apple's Mail Drop service.

NOTE: This recommendation only applies if an institutionally configured mail account resides on the iOS device.

Rationale:

Permitting attachment uploads to Mail Drop, which is outside organizational control, presents a data exfiltration path.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.
4. In the right windowpane, verify that the checkbox for `Allow Mail Drop` is `unchecked`.

From the device, there is no audit mechanism.

Remediation:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left windowpane, click on the `Mail` tab.
4. In the right windowpane, uncheck the checkbox for `Allow Mail Drop`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3 <u>Configure Data Access Control Lists</u>** Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	**14.6 <u>Protect Information through Access Control Lists</u>** Protect all information stored on systems 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.	●	●	●

3.8 Notifications

3.8.1 (L1) Ensure "Notification Settings" are configured for all "Managed Apps" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the configuration of notification settings on a per-application basis.

Rationale:

Notifications may include sensitive data or might allow for privileged actions to take place. All managed applications must include explicit notification settings in order to address these concerns.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Notifications` tab.
4. In the right window pane, verify that each managed app includes a configuration entry.

Or, from the device:

1. Tap `Settings`.
2. Tap `Notifications`.
3. Verify that managed apps are grayed out to indicate that their notification settings are managed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Notifications` tab.
4. In the right window pane, click `Configure` and/or click the + to add notification settings on a per-app basis.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.9 Lock Screen Message

3.9.1 (L1) Ensure "If Lost, Return to..." Message is "Configured" (Manual)

Profile Applicability:

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to configuring a lock screen message.

Rationale:

A lock screen message will allow an honest bystander to more easily return a lost device.

This message need not identify the owner by name, but should reference a phone number or email address to contact (for example, the help desk of an organization).

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Lock Screen Message` tab.
4. In the right window pane, verify that in the `"If Lost, Return to..." Message` is configured appropriately.

Or, from the device:

1. Wake the device.
2. Verify on the lock screen that an appropriate message is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Lock Screen Message` tab.
4. In the right window pane, in the `"If Lost, Return to..." Message` field, configure an appropriate message.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4 Additional Recommendations

This section provides both level 1 and level 2 recommendations for configuring iOS and iPadOS devices. These recommendations are not configurable via a configuration profile. They are accessible on the device either locally or through certain Mobile Device Management (MDM) solutions.

4.1 Privacy & Security

4.1.1 (L1) Review Manage Sharing & Access (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

Managing Sharing & Access is a new feature available with iOS 16, which allows via a wizard to review what is being shared with people and apps to determine if current settings are adequate or if some access needs to be revoked. It also allows to review the settings related to a user's Apple ID.

Rationale:

By regularly reviewing what is being shared with apps and people, and by reviewing the Apple ID settings, users can ensure sharing settings are accurate and fit for purpose as well as their Apple ID is kept safe.

Audit:

From the device:

1. Tap Settings.
2. Tap Privacy & Secuurity.
3. Tap Safety Check.
4. Tap Manage Sharing & Access.
5. Tap Continue.
6. Go through the 3 steps to review the settings.
7. Tap Done at the end of the procedure.

Remediation:

From the device:

1. Tap Settings.
2. Tap Privacy & Secuurity.
3. Tap Safety Check.
4. Tap Manage Sharing & Access.
5. Tap Continue.
6. Remove sharing from any applications or people that are outside your organization's requirements
7. Tap Done at the end of the procedure.

References:

1. https://support.apple.com/en-lb/guide/personal-safety/ips16ea6f2fe/1.0/web/1.0#ips3a9e8e23f
2. https://support.apple.com/en-lb/guide/personal-safety/welcome/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

4.1.2 (L2) Review Emergency Reset (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

- Level 2 - Institutionally-Owned Devices

Description:

Emergency Reset is a one-tap option that allows to protect a user by revoking everything an iOS device is sharing all people and apps; this includes things like location information, home data, photo albums and more.

Emergency Reset also allows to remove all emergency contacts and reset user's Apple ID and password, so no one can log into their account.

Rationale:

Emergency Reset is designed for people who are experiencing or at risk of domestic abuse, but it's also useful for anyone who has ever shared their location or data with partners in the past. The tool is a centralized dashboard of controls meant to simplify resetting privacy permissions, revoking location access and auditing data sharing.

Monitoring smartphones is a common tactic in domestic-abuse situations because it takes advantage of everyday tools, such as iCloud or location sharing. By cutting off an abuser's access to a device it is possible mitigating the risks of being stalked or exposed.

Audit:

There is no way to audit `Emergency Reset` since it is not a state that can be set.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `Privacy & Secuurity`.
3. Tap `Safety Check`.
4. Tap `Emergency Reset`.
5. Tap `Start Emergency Reset`.
6. Follow the onscreen instructions until the procedure is complete.

References:

1. https://support.apple.com/en-lb/guide/personal-safety/ips16ea6f2fe/1.0/web/1.0#ips3a9e8e23f
2. https://support.apple.com/en-lb/guide/personal-safety/welcome/web

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		🟠	🔵
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		🟠	🔵

4.1.3 (L2) Review Lockdown Mode (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

- Level 2 - Institutionally-Owned Devices

Description:

Lockdown Mode is a new operational model made available with iOS. It ensures a high level of security by limiting or disabling a nummber of features of the device

Lockdown Mode blocks most attachment types in Messages, blocks FaceTime calls from non-contacts, limits web browsing functions, prevents configuration profiles from being installed, and more, with a full list available in our Lockdown article.

Rationale:

Lockdown Mode is meant for users who can be targeted by sophisticated cyberattacks (such as activists, journalists and others) and as such requires an additional level of security.

Impact:

Lockdown Mode is not for the average user and is meant for individual operating in very specific and risky circumstances. When Lockdown Mode is enabled the device doesn't work as usual: certain apps, websites and features are strictly limited for security and some experiences might not be available at all.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `Privacy & Security`.
3. Under Security, verify the status of Lockdown Mode.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `Privacy & Security`.
3. Tap `Lockdown Mode`.
4. Tap `Turn On Lockdown Mode`.
5. Tap `Turn On Lockdown Mode`.
6. Tap `Turn On & Restart`.
7. Enter the device passcode.

References:

1. https://support.apple.com/en-us/HT212650
2. https://techcrunch.com/2023/04/18/apple-lockdown-mode-iphone-nso-pegasus/?guccounter=1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.1.4 (L2) Ensure "App Privacy Report" is enabled (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

- Level 2 - Institutionally-Owned Devices

Description:

App Privacy Report is a tool that provides details about how often apps access your data, such as location, camera, microphone and more. The tool also returns information about each app network activity and website network activity, as well as the web domains that all apps contact most frequently.

Rationale:

By regularly using App Privacy Report, users can have a comprehensive picture of how the apps behave and how they use their data.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `Privacy & Security`.
3. Tap `App Privacy Report`.
4. Verify the status of App Privacy Report.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `Privacy & Security`.
3. Tap the services you want to disable or modify
4. Set any/all applications to the settings for your organization's requirements

References:

1. https://support.apple.com/en-us/HT212958

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.1.5 (L2) Review Airprint (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to Apple's AirPrint, a feature for printing without installing printer-specific drivers.

Rationale:

AirPrint does not enforce managed boundaries for printers. This allows the device to connect to any AirPrint compatible printer, which may result in data leakage.

Impact:

End users may be inconvenienced by disabling AirPrint on their personal devices since they may already be using Airprint compatible printers in their homes.

Audit:

From the Configuration Profile:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, verify that under the tab `Functionality`, that the checkbox for `Allow AirPrint (supervised only)` is `unchecked`.

Or, from the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `VPN & Device Management`.
4. Tap `<_Profile Name_>`.
5. Tap `Restrictions`.
6. Confirm `AirPrint is not allowed` is displayed.

Remediation:

1. Open Apple Configurator.
2. Open the Configuration Profile.
3. In the left window pane, click on the `Restrictions` tab.
4. In the right window pane, under the tab `Functionality`, `uncheck` the checkbox for `Allow AirPrint (supervised only)`.
5. Deploy the Configuration Profile.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.1.6 (L2) Ensure "Stolen Device Protection" Is Enabled (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

Description:

With the release of iOS and iPadOS 17.3, Apple added the ability to restrict when a passcode can be reset. Turning this on will protect a user if their phone is stolen and the thief has obtained the user's passcode. If the passcode is compromised, a user's iCloud credentials can be reset or altered, giving access to the user's AppleID.

To access your significant locations follow this guide: [Delete significant locations on iPhone](#).

To learn more about what access to an AppleID allows: [Where can I use my Apple ID?](#)

Rationale:

Requiring a user to be in a significant location to reset the passcode can hinder (or thwart) the takeover of a user's identity, through iCloud, in the case of a stolen device.

Impact:

This could cause an issue for the user if they are trying to change their passcode outside of their significant location(s).

Audit:

From the device:

1. Tap `Settings`
2. Tap `Face ID & Passcode`
3. Enter the passcode
4. Tap `Stolen Device Protection`.
5. Verify `Stolen Device Protection` is enabled.

Remediation:

From the device:

1. Tap `Settings`
2. Tap `Face ID & Passcode`
3. Enter the passcode
4. Tap `Stolen Device Protection`
5. Enable `Stolen Device Protection`

References:

1. https://9to5mac.com/2024/01/22/turn-on-iphone-stolen-device-protection/
2. https://tidbits.com/2024/01/25/turn-on-stolen-device-protection-in-ios-17-3/
3. https://news.ycombinator.com/item?id=34936015

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 <u>Use Unique Passwords</u> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

4.2 (L1) Ensure device is not obviously jailbroken or compromised (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to inspecting a device for the presence of the most common jailbreak indicator.

Rationale:

Apple imposes certain restrictions on which apps can be installed on a device. Further, no app can gain access to information and data on the device or another app without being given authorization. This restricts the potential risk of unauthorized access by an app due to the limited administrative rights allowed by Apple. A compromised iOS device, both unintentionally in the event of a malicious actor and willingly as for jailbroken devices, may circumvent the above restrictions and in doing so may execute arbitrary code, compromise configuration profile requirements, or open the device to exploits that are otherwise not possible.

Audit:

The ways a device is compromised change over time, thus it may prove to be hard detecting a compromised device. However, there are some indicators that are suspiscious and might mean an iOS device is no longer genuine.

1. Suspicious apps are installed on the device.
2. High data usage.
3. The device is hot or overheats.
4. High battery drain.
5. Poor overall performance.
6. Unrecongnized calls/texts.

For jailbroken devices, the additional checks below can be run:

1. From the Home Screen, swipe down to open Spotlight.
2. Enter `Cydia`, `Sileo`, and `checkra1n`.
3. Confirm every time that Spotlight results do not return any of the apps above.

Remediation:

Restore the iOS to a known good state from a trusted computer:

1. Open iTunes.
2. Connect the iOS device to the computer with a USB cable.
3. Select your iOS device within iTunes.
4. Select Restore iPhone/iPad.
5. After restoration, set up as a new device or restore from a known good backup.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**2.2** <u>Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	🟢	🟠	🔵
v7	**2.2** <u>Ensure Software is Supported by Vendor</u> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	🟢	🟠	🔵

4.3 (L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the automatic installation of operating system updates.

Rationale:

System updates may patch software vulnerabilities, therefore it is important that devices are kept up-to-date.

Impact:

In the following circumstances automatic updates should be kept disabled:

- If the organization leverages third-party tools to manage software updates for Apple devices,
- If the organization has a strict patch management process, which involves testing the software updates on pilot devices before an exhaustive roll-out.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Updates`
4. Tap `Automatic Updates`.
5. Verify that `Download iOS Updates` and `Install iOS Updates` are enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Updates`
4. Tap `Automatic Updates`.
5. Enable `Download iOS Updates` and `Install iOS Updates`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.3 <u>Perform Automated Operating System Patch Management</u>** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	🟢	🟠	🔵
v7	**3.4 <u>Deploy Automated Operating System Patch Management Tools</u>** Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	🟢	🟠	🔵

4.4 (L1) Ensure "Software Update" returns "Your software is up to date." (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to updating and upgrading the operating system of a given device.

Rationale:

An up-to-date operating system provides the best possible protection against the execution of malicious code.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. Verify that `iOS is up to date.` is returned.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `General`.
3. Tap `Software Update`.
4. Tap `Install` or `Download and Install` and then allow device to complete the installation.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.3 Perform Automated Operating System Patch Management** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	**7.4 Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	**3.4 Deploy Automated Operating System Patch Management Tools** Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
v7	**3.5 Deploy Automated Software Patch Management Tools** Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

4.5 (L1) Review "iCloud Private Relay" settings (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

iCloud Private Relay is a service offered by Apple as part of an iCloud+ subscription. It allows users on iOS 15, iPadOS 15, macOS Monterey, or later versions of iOS, iPadOS, and macOS to browse the Web more privately by hiding the user's actual IP address.

The service makes use of a multi-hop architecture whereby a user's requests are sent through two separate internet relays, operated by different entities, that replace a user's original IP address.

The user's IP address is visible to the network provider and to the first relay, which is operated by Apple. The DNS records are encrypted, so neither party can see the address of the website the user is trying to visit. The second relay, which is operated by a third-party content provider, generates a temporary IP address, decrypts the name of the website, and connects to the site. By doing so, no single party — including Apple — can view or collect the details of a user's browsing activity or unencrypted activity in applications.

Rationale:

While browsing the Web, information contained in the Web traffic, such as DNS records and IP address, can be seen by a network provider and by any websites visited. This information could be used to determine a user's identity and build a profile of their location and browsing history.

Hiding this information prevents the tracking and profiling of users, resulting in an increased level of privacy while browsing the Web.

Impact:

iCloud Private Relay only protects connections on public internet servers, instructing the device to try to access the servers directly over the local network. Some entities or enterprises, however, might be required to audit all network traffic by policy. In this case, it is possible to block access to Private Relay. Should iCloud Private Relay be blocked, the user will be alerted that they need to either disable the feature or choose another network. In this scenario, users will still be able to use the service when they are not connected to their corporate network.

The fastest and most reliable way to do this is to return a negative answer from the network's DNS resolver, preventing DNS resolution for the mask.icloud.com and mask-h2.icloud.com hostnames necessary for Private Relay traffic.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `iCloud`.
4. Tap `Private Relay`.
5. Verify that `Private Relay` is enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `iCloud`.
4. Tap `Private Relay`.
5. Enable `Private Relay`.

References:

1. https://www.apple.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	**4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software** Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	**9.2 Ensure Only Approved Ports, Protocols and Services Are Running** Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.6 (L1) Review "Mail Privacy Protection" settings (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices

- Level 1 - Institutionally-Owned Devices

Description:

Mail Privacy Protection helps protect user privacy by preventing email senders from learning information about the activity they engage with using the Mail application. When turned on, this feature hides user IP addresses.

Rationale:

By enabling Mail Privacy, senders cannot build a profile of a user's online activity or determine their location. Such a feature also prevents senders from seeing if users have opened the email they sent.

Hiding user IP addresses prevents user tracking and profiling, which results in an increased level of privacy while using the Mail app.

Impact:

Some entities or enterprises might be required to audit all network traffic by policy. In this case, it is possible to block access to Mail Privacy Protection. The fastest and most reliable way to do this is to return a negative answer from the network's DNS resolver, preventing DNS resolution for the mask.icloud.com and mask-h2.icloud.com hostnames necessary for Mail Privacy Protection traffic.

In this scenario, users will still be able to use the service when they are not connected to their corporate network.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `Mail`.
3. Tap `Privacy Protection`.
4. Verify that `Protect Mail Activity` is enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `Mail`.
3. Tap `Privacy Protection`.
4. Enable `Protect Mail Activity`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.7 (L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled" (Manual)

Profile Applicability:

- Level 1 - End-User Owned Devices
- Level 1 - Institutionally-Owned Devices

Description:

This recommendation pertains to the automatic installation of application updates.

Rationale:

Application updates may patch software vulnerabilities.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `App Store`.
3. Verify that under `AUTOMATIC DOWNLOADS`, `App Updates` is enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `iTunes & App Store`.
3. Under `AUTOMATIC DOWNLOADS`, enable `App Updates`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**7.4 Perform Automated Application Patch Management** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	**3.5 Deploy Automated Software Patch Management Tools** Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

4.8 (L1) Ensure "Find My iPhone/iPad" is set to "Enabled" on end user-owned devices (Automated)

Profile Applicability:

- Level 1 - End-User Owned Devices

Description:

This recommendation pertains to remote device locating, locking, and erasure by the end user.

Rationale:

The ability to locate, lock, and erase a device remotely helps mitigate the impact of device theft and loss, as well as the likelihood of permanent loss.

This is only recommended for end user-owned devices. Institutionally-owned devices should not be erasable by end users.

Impact:

Evidence may be destroyed if an end user performs an erase.

Audit:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `Find My`.
4. Verify `Find My iPhone`, `Find My Network` and `Send Last Location` are enabled.

Remediation:

From the device:

1. Tap `Settings`.
2. Tap `<_The User's Name_>` where `Apple ID, iCloud, iTunes & App Store` is displayed beneath.
3. Tap `Find My`.
4. Enable `Find My iPhone`, `Find My Network` and `Send Last Location`.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.13 Deploy a Data Loss Prevention Solution** Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			●
v7	**14.5 Utilize an Active Discovery Tool to Identify Sensitive Data** Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.			●

4.9 (L2) Ensure the latest iOS device architecture is used by high-value targets (Manual)

Profile Applicability:

- Level 2 - End-User Owned Devices

- Level 2 - Institutionally-Owned Devices

Description:

This recommendation pertains to the physical device(s) used by high-value targets.

Rationale:

Physical security exploits against iOS devices are rarely demonstrated within two years of the release of the underlying architecture. For users whose physical iOS device(s) may be targeted, it is prudent to use the most recently released architecture.

Audit:

Ensure the device(s) deployed to high-value targets are of the latest generation architecture.

Remediation:

Replace the device(s).
As of publication, the latest iOS device architectures are:

- iPhone 13 and iPhone 13 Mini using the Apple A15 Bionic processor
- iPhone 13 Pro and iPhone 13 Pro Max using the Apple A15 Bionic processor
- iPad Mini 8.3" using the Apple A15 Bionic processor
- iPad 10.2" using the Apple A13 Bionic processor
- iPad Air 10.9" using the Apple A14 Bionic processor
- iPad Pro 11" and 12.9" using the Apple M1 processor

Additional Information:

Apple provides the following material on identifying iOS device hardware. For iPhone, see: https://support.apple.com/en-us/HT201296. For iPad, see: https://support.apple.com/en-us/HT201471.

The term *high-value targets* is being used to refer to users who may be likely to experience a physical-level device attack. Examples include:

- Politicians
- Journalists
- Activists
- Civilian government or military personnel
- Business executives
- Wealthy individuals

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**1.1 Establish and Maintain Detailed Enterprise Asset Inventory** Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	●	●	●
v7	**1.4 Maintain Detailed Asset Inventory** Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Benchmark Guidance**		
2	**Configuration Profile Recommendations for End User-Owned Devices**		
2.1	**General**		
2.1.1	(L1) Ensure a "Consent Message" has been "Configured" (Automated)	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always" (Manual)	☐	☐
2.2	**Restrictions**		
2.2.1	**Functionality**		
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled" (Automated)	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled" (Automated)	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled" (Automated)	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled" (Automated)	☐	☐
2.2.1.5	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled" (Manual)	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled" (Automated)	☐	☐
2.2.1.7	(L1) Ensure "Force automatic date and time" is set to "Enabled" (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled" (Automated)	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled" (Automated)	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled" (Automated)	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled" (Automated)	☐	☐
2.2.1.12	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled" (Manual)	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled" (Automated)	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled" (Automated)	☐	☐
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled" (Automated)	☐	☐
2.2.2	**Applications**		
2.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled" (Automated)	☐	☐
2.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only" (Automated)	☐	☐
2.3	**Domains**		
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured" (Manual)	☐	☐
2.4	**Passcode**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled" (Automated)	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled" (Manual)	☐	☐
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater (Automated)	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less (Automated)	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately" (Automated)	☐	☐
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6" (Automated)	☐	☐
2.5	**Wi-Fi**		
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured" (Manual)	☐	☐
2.6	**VPN**		
2.6.1	(L1) Ensure "VPN" is "Configured" (Manual)	☐	☐
2.7	**Mail**		
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled" (Automated)	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled" (Automated)	☐	☐
2.8	**Notifications**		
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps" (Manual)	☐	☐
3	**Configuration Profile Recommendations for Institutionally-Owned Devices**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1	**General**		
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never" (Automated)	☐	☐
3.2	**Restrictions**		
3.2.1	**Functionality**		
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled" (Manual)	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled" (Automated)	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled" (Automated)	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled" (Automated)	☐	☐
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled" (Automated)	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings (Automated)	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled" (Automated)	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled" (Automated)	☐	☐
3.2.1.9	(L2) Ensure "Allow network drive access in Files app" is set to "Disabled" (Automated)	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled" (Automated)	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled" (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled" (Automated)	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled" (Automated)	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled" (Manual)	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled" (Automated)	☐	☐
3.2.1.16	(L1) Ensure "Allow adding VPN configurations" is set to "Disabled" (Automated)	☐	☐
3.2.1.17	(L1) Ensure "Force automatic date and time" is set to "Enabled" (Manual)	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled" (Automated)	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled" (Automated)	☐	☐
3.2.1.20	(L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled" (Automated)	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled" (Automated)	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled" (Automated)	☐	☐
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled" (Automated)	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled" (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled" (Manual)	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled" (Automated)	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled" (Automated)	☐	☐
3.2.1.28	(L1) Ensure "Allow setting up new nearby devices" is set to "Disabled" (Automated)	☐	☐
3.2.1.29	(L1) Ensure "Allow proximity based password sharing requests" is set to "Disabled" (Automated)	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled" (Manual)	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled" (Automated)	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled" (Automated)	☐	☐
3.2.2	**Apps**		
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled" (Automated)	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only" (Automated)	☐	☐
3.3	**Domains**		
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured" (Manual)	☐	☐
3.4	**Passcode**		
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled" (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled" (Manual)	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater (Automated)	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less (Automated)	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately" (Automated)	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6" (Automated)	☐	☐
3.5	**Wi-Fi**		
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured" (Manual)	☐	☐
3.6	**VPN**		
3.6.1	(L1) Ensure "VPN" is "Configured" (Manual)	☐	☐
3.7	**Mail**		
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled" (Automated)	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled' (Automated)	☐	☐
3.8	**Notifications**		
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps" (Manual)	☐	☐
3.9	**Lock Screen Message**		
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured" (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	**Additional Recommendations**		
4.1	**Privacy & Security**		
4.1.1	(L1) Review Manage Sharing & Access (Manual)	☐	☐
4.1.2	(L2) Review Emergency Reset (Manual)	☐	☐
4.1.3	(L2) Review Lockdown Mode (Manual)	☐	☐
4.1.4	(L2) Ensure "App Privacy Report" is enabled (Manual)	☐	☐
4.1.5	(L2) Review Airprint (Manual)	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled (Manual)	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised (Manual)	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled" (Manual)	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date." (Manual)	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings (Manual)	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings (Manual)	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled" (Manual)	☐	☐
4.8	(L1) Ensure "Find My iPhone/iPad" is set to "Enabled" on end user-owned devices (Automated)	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets (Manual)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.5	(L2) Review Airprint	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.5	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.7	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.12	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐

	Recommendation	Set Correctly	
		Yes	No
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
2.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.16	(L1) Ensure "Allow adding VPN configurations" is set to "Disabled"	☐	☐
3.2.1.17	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled"	☐	☐
3.2.1.20	(L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
3.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐
4.1.1	(L1) Review Manage Sharing & Access	☐	☐
4.1.2	(L2) Review Emergency Reset	☐	☐
4.1.3	(L2) Review Lockdown Mode	☐	☐
4.1.4	(L2) Ensure "App Privacy Report" is enabled	☐	☐
4.1.5	(L2) Review Airprint	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.5	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.7	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.12	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
2.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.9	(L2) Ensure "Allow network drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.16	(L1) Ensure "Allow adding VPN configurations" is set to "Disabled"	☐	☐
3.2.1.17	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled"	☐	☐
3.2.1.20	(L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.28	(L1) Ensure "Allow setting up new nearby devices" is set to "Disabled"	☐	☐
3.2.1.29	(L1) Ensure "Allow proximity based password sharing requests" is set to "Disabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
3.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐
4.1.1	(L1) Review Manage Sharing & Access	☐	☐
4.1.2	(L2) Review Emergency Reset	☐	☐
4.1.3	(L2) Review Lockdown Mode	☐	☐
4.1.4	(L2) Ensure "App Privacy Report" is enabled	☐	☐
4.1.5	(L2) Review Airprint	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.8	(L1) Ensure "Find My iPhone/iPad" is set to "Enabled" on end user-owned devices	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation	Set Correctly	
	Yes	No
No unmapped recommendations to CIS Controls v7	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled"	☐	☐
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.9	(L2) Ensure "Allow network drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐
4.1.5	(L2) Review Airprint	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.5	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.7	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.12	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
2.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.9	(L2) Ensure "Allow network drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.16	(L1) Ensure "Allow adding VPN configurations" is set to "Disabled"	☐	☐
3.2.1.17	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled"	☐	☐
3.2.1.20	(L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.29	(L1) Ensure "Allow proximity based password sharing requests" is set to "Disabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
3.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐
4.1.1	(L1) Review Manage Sharing & Access	☐	☐
4.1.2	(L2) Review Emergency Reset	☐	☐
4.1.3	(L2) Review Lockdown Mode	☐	☐
4.1.4	(L2) Ensure "App Privacy Report" is enabled	☐	☐
4.1.5	(L2) Review Airprint	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
2.1.1	(L1) Ensure a "Consent Message" has been "Configured"	☐	☐
2.1.2	(L1) Ensure "Controls when the profile can be removed" is set to "Always"	☐	☐
2.2.1.1	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
2.2.1.2	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
2.2.1.3	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
2.2.1.4	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
2.2.1.5	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
2.2.1.6	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
2.2.1.7	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
2.2.1.8	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
2.2.1.9	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐
2.2.1.10	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
2.2.1.11	(L2) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
2.2.1.12	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
2.2.1.13	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
2.2.1.14	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.2.1.15	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
2.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
2.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
2.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
2.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
2.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
2.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
2.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
2.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
2.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐
2.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
2.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
2.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
2.7.2	(L1) Ensure "Allow Mail Drop" is set to "Disabled"	☐	☐
2.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.1.1	(L1) Ensure "Controls when the profile can be removed" is set to "Never"	☐	☐
3.2.1.1	(L2) Ensure "Allow screenshots and screen recording" is set to "Disabled"	☐	☐
3.2.1.2	(L1) Ensure "Allow voice dialing while device is locked" is set to "Disabled"	☐	☐
3.2.1.3	(L1) Ensure "Allow Siri while device is locked" is set to "Disabled"	☐	☐
3.2.1.4	(L1) Ensure "Allow iCloud backup" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.5	(L1) Ensure "Allow iCloud documents & data" is set to "Disabled"	☐	☐
3.2.1.6	(L1) Review "Allow iCloud Keychain" settings	☐	☐
3.2.1.7	(L1) Ensure "Allow managed apps to store data in iCloud" is set to "Disabled"	☐	☐
3.2.1.8	(L2) Ensure "Allow USB drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.9	(L2) Ensure "Allow network drive access in Files app" is set to "Disabled"	☐	☐
3.2.1.10	(L1) Ensure "Force encrypted backups" is set to "Enabled"	☐	☐
3.2.1.11	(L1) Ensure "Allow personalized ads delivered by Apple" is set to "Disabled"	☐	☐
3.2.1.12	(L1) Ensure "Allow Erase All Content and Settings" is set to "Disabled"	☐	☐
3.2.1.13	(L2) Ensure "Allow users to accept untrusted TLS certificates" is set to "Disabled"	☐	☐
3.2.1.14	(L1) Ensure "Allow trusting new enterprise app authors" is set to "Disabled"	☐	☐
3.2.1.15	(L1) Ensure "Allow installing configuration profiles" is set to "Disabled"	☐	☐
3.2.1.16	(L1) Ensure "Allow adding VPN configurations" is set to "Disabled"	☐	☐
3.2.1.17	(L1) Ensure "Force automatic date and time" is set to "Enabled"	☐	☐
3.2.1.18	(L2) Ensure "Allow modifying cellular data app settings" is set to "Disabled"	☐	☐
3.2.1.19	(L1) Ensure "Allow USB accessories while the device is locked" is set to "Disabled"	☐	☐
3.2.1.20	(L2) Ensure "Allow pairing with non-Configurator hosts" is set to "Disabled"	☐	☐
3.2.1.21	(L1) Ensure "Allow documents from managed sources in unmanaged destinations" is set to "Disabled"	☐	☐
3.2.1.22	(L1) Ensure "Allow documents from unmanaged sources in managed destinations" is set to "Disabled"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2.1.23	(L1) Ensure "Treat AirDrop as unmanaged destination" is set to "Enabled"	☐	☐
3.2.1.24	(L1) Ensure "Allow Handoff" is set to "Disabled"	☐	☐
3.2.1.25	(L1) Ensure "Allow sending diagnostic and usage data to Apple" is set to "Disabled"	☐	☐
3.2.1.26	(L1) Ensure "Require Touch ID / Face ID authentication before AutoFill" is set to "Enabled"	☐	☐
3.2.1.27	(L1) Ensure "Force Apple Watch wrist detection" is set to "Enabled"	☐	☐
3.2.1.28	(L1) Ensure "Allow setting up new nearby devices" is set to "Disabled"	☐	☐
3.2.1.29	(L1) Ensure "Allow proximity based password sharing requests" is set to "Disabled"	☐	☐
3.2.1.30	(L1) Ensure "Allow password sharing (supervised only)" is set to "Disabled"	☐	☐
3.2.1.31	(L1) Ensure "Show Control Center in Lock screen" is set to "Disabled"	☐	☐
3.2.1.32	(L1) Ensure "Show Notification Center in Lock screen" is set to "Disabled"	☐	☐
3.2.2.1	(L1) Ensure "Force fraud warning" is set to "Enabled"	☐	☐
3.2.2.2	(L1) Ensure "Accept cookies" is set to "From websites I visit" or "From current website only"	☐	☐
3.3.1	(L1) Ensure "Managed Safari Web Domains" is "Configured"	☐	☐
3.4.1	(L1) Ensure "Allow simple value" is set to "Disabled"	☐	☐
3.4.2	(L2) Ensure "Require alphanumeric value" is set to "Enabled"	☐	☐
3.4.3	(L1) Ensure "Minimum passcode length" is set to a value of "6" or greater	☐	☐
3.4.4	(L1) Ensure "Maximum Auto-Lock" is set to "2 minutes" or less	☐	☐
3.4.5	(L1) Ensure "Maximum grace period for device lock" is set to "Immediately"	☐	☐
3.4.6	(L1) Ensure "Maximum number of failed attempts" is set to "6"	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.5.1	(L1) Ensure "Disable Association MAC Randomization" is "Configured"	☐	☐
3.6.1	(L1) Ensure "VPN" is "Configured"	☐	☐
3.7.1	(L1) Ensure "Allow user to move messages from this account" is set to "Disabled"	☐	☐
3.7.2	(L2) Ensure 'Allow Mail Drop' is set to 'Disabled'	☐	☐
3.8.1	(L1) Ensure "Notification Settings" are configured for all "Managed Apps"	☐	☐
3.9.1	(L1) Ensure "If Lost, Return to..." Message is "Configured"	☐	☐
4.1.1	(L1) Review Manage Sharing & Access	☐	☐
4.1.2	(L2) Review Emergency Reset	☐	☐
4.1.3	(L2) Review Lockdown Mode	☐	☐
4.1.4	(L2) Ensure "App Privacy Report" is enabled	☐	☐
4.1.5	(L2) Review Airprint	☐	☐
4.1.6	(L2) Ensure "Stolen Device Protection" Is Enabled	☐	☐
4.2	(L1) Ensure device is not obviously jailbroken or compromised	☐	☐
4.3	(L1) Ensure "Install iOS Updates" of "Automatic Updates" is set to "Enabled"	☐	☐
4.4	(L1) Ensure "Software Update" returns "Your software is up to date."	☐	☐
4.5	(L1) Review "iCloud Private Relay" settings	☐	☐
4.6	(L1) Review "Mail Privacy Protection" settings	☐	☐
4.7	(L1) Ensure "Automatic Downloads" of "App Updates" is set to "Enabled"	☐	☐
4.8	(L1) Ensure "Find My iPhone/iPad" is set to "Enabled" on end user-owned devices	☐	☐
4.9	(L2) Ensure the latest iOS device architecture is used by high-value targets	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation	Set Correctly	
	Yes	No
No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version
September 20, 2024	1.0.0	Initial Draft Release
October 7, 2024	1.0.0	Initial Release