jamf

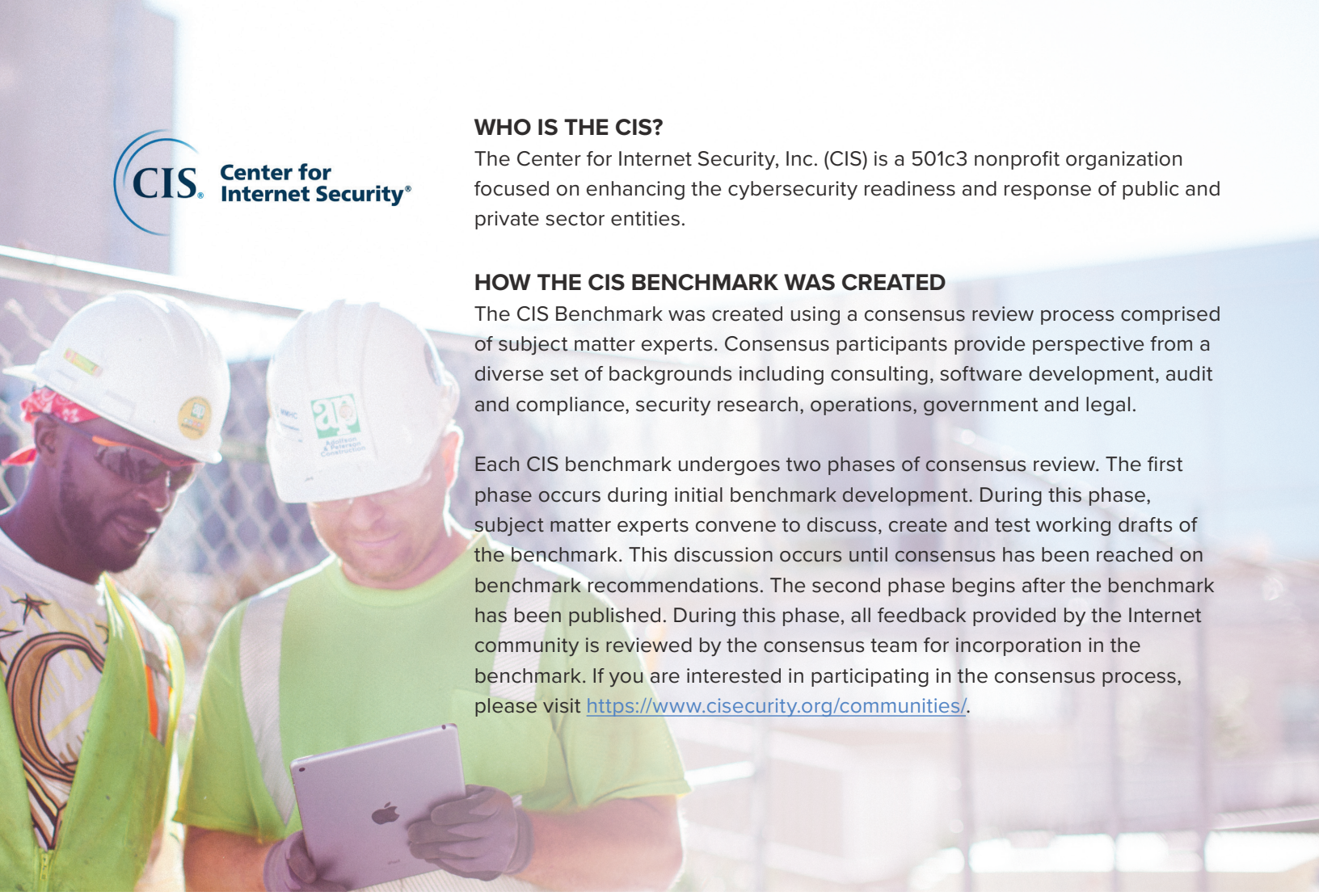
WHITE PAPER

Security Checklist

Implementing the Center for Internet Security Benchmark

Recommendations for securing iPad and iPhone.

The Center for Internet Security (CIS) benchmark for iOS is widely regarded as a comprehensive checklist for organizations to follow to secure iPad and iPhone devices. This white paper explains how to implement the independent organization's recommendations.



WHO IS THE CIS?

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities.

HOW THE CIS BENCHMARK WAS CREATED

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

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

CIS Management Basics

WHAT IS MDM?

Mobile device management (MDM) is Apple's built-in management framework for iOS, iPadOS, macOS and tvOS. Jamf Now is the standard solution for Apple MDM.

WHAT ARE BLUEPRINTS?

Blueprints define settings on Apple devices and are distributed to the devices via Jamf Now.

WHAT IS APNs?

Apple Push Notification service (APNs) is required for iPad and iPhone management. Read **here** to learn more about APNs.

DEVICE OWNERSHIP

Security requirements are different based on the organization's technology model: personally-owned via a bring your own device (BYOD) initiative or institutionally-owned and distributed to users.

WHAT IS SUPERVISION?

Supervision provides a deeper level of iPhone and iPad management once devices are enrolled into management via Apple's deployment programs, Automated Device Enrollment and Volume Purchasing.

Securing Company-Owned Devices

A recent survey found that 74 percent of enterprise employees would prefer a company-issued device over a personally-owned device.* Jamf Now helps organizations securely implement their company-owned iPhone and iPad program, and empowers them to streamline distribution and management of Apple devices.

CIS Recommendations

Setup:

- Ensure the profile can be removed.

Functionality:

- Disable screenshots and screen recording.
- Disable Siri while device is locked.
- Disable iCloud backup.
- Disable iCloud documents and data.
- Disable iCloud Keychain.
- Disable managed apps to store data in iCloud.
- Enable force encryption backups.
- Disable allow all content and settings.
- Disable allow modifying cellular data app settings.
- Disable allow pairing with non-Configurator hosts.
- Disable allow documents from managed sources in unmanaged destinations.
- Disable allow documents from unmanaged sources in managed destinations.
- Enable treat AirDrop as unmanaged destination.
- Disable allow setting up a new nearby device.
- Disable show Notification Center in Lock screen.

Domains:

- Configure managed Safari web domains.

Passcodes:

- Disable allow simple value.
- Minimum passcode length is set to “6” or greater.
- Maximum Auto-Lock is set to “2 minutes” or less.
- Maximum grace period for device lock is set to “Immediately”.
- Maximum number of failed attempts is set to “6”.

VPN:

- Ensure VPN is “Configured”.

Mail:

- Set up a user’s email account with an Email profile.

Notifications:
- Configure notification settings for all managed apps.

Lock Screen Message:
- Configure “If Lost, Return to...” message.

Features in Jamf Now

Jamf Now allows you to set, enable and/or disable over 75 features and deploy them through Blueprints. A few of these settings require the iPhone or iPad to be supervised during enrollment. Please review the following from Apple for more information on **iPad and iPhone supervision**.

With the Plus Plan, Jamf Now also allows organizations to set a personalized Lock Screen message to ensure devices are safely returned and not unlocked and tampered with. All of the Restrictions and features empower every organization to customize how they set up their devices to fit each of their team’s needs and device usage. Use the above recommendations as a guide when creating your plan.

Source: **The Impact of Device Choice on the Employee Experience**

Securing BYOD and Personally-Owned Devices

Jamf Now helps organizations securely remove the burden of multiple devices for their employees, and empowers them to utilize one device for both work and home. If your organization is allowing personally-owned devices or BYOD, making sure that the devices are under the umbrella of your MDM helps keep your company and customer data secure.

CIS Recommendations

Setup:
- Set a consent message and description for the enrollment profile.
- Ensure the profile can be removed.

Functionality:
- Disable Siri while device is locked.
- Disable managed apps to store data in iCloud.
- Enable force encryption backups.
- Disable documents managed from sources in unmanaged destinations.
- Disable documents from unmanaged sources in managed destinations.
- Enable treat AirDrop as unmanaged destination.
- Disable show Control Center in Lock screen.
- Disable show Notification Center in Lock screen.

Apps:
- Accept cookies is set to “From websites I visit” or “From current website only”.

Domains:
- Configure managed Safari web domains.

Passcodes:
- Disable allow simple value.
- Minimum passcode length is set to “6” or greater.
- Maximum Auto-Lock is set to “2 minutes” or less.
- Maximum grace period for device lock is set to “Immediately”.
- Maximum number of failed attempts is set to “6”.

VPN:
- Ensure VPN is “Configured”.

Mail:
- Set up a user’s email account with an Email profile.
- Disable allow user to move message from this account.

Features in Jamf Now

Jamf Now BYOD solution allows you to deploy the designated enrollment profile, as well as a simple process for former employees to remove the BYOD profile if they leave the organization or the program.

If your organization is implementing a BYOD program to allow your users to use the devices they are comfortable with, the above recommendations are a great place to start crafting your plan. With BYOD programs, security takes an even greater priority because you know the device will be used for more than work functions. Making sure you protect your data from potential outside threats is crucial.

Additional Considerations

Jamf Now helps organizations go beyond device management and Blueprints by ensuring devices are always running the latest software and not leaving the door open to malicious attacks.

CIS Recommendations:

- Ensure the iPhone and iPad device is not obviously jailbroken.
- Keep software up to date.
- Enable automatic downloads of app updates.
- On BYOD devices only, enable Find My iPad and/or Find My iPhone.
- Ensure the latest iOS update is running on the device.

Features in Jamf Now

Jamf Now offers day-zero support for iOS and iPadOS ensuring the newest software is always supported. On-demand access is granted for users, all without them ever submitting a support ticket. If a device is lost or stolen, Jamf Now can safely lock, wipe and reset the device, ensuring company, customer and personal data are never exposed.

Better Device Security Starts Here

Jamf Now makes it easy to implement, follow and deploy the independent organization Center for Internet Security's Apple iOS benchmarks.

Put this guide to practice in your environment by **creating your free account**. First 3 devices are free - Forever!

jamf

To learn more about how Jamf Now can make an impact on your Mac, iPhone and iPad management, visit **www.jamf.com/products/jamf-now/**.