How to Create a Mobile Device Security Policy, With Template

TechTarget

How to Create a Mobile Device Security Policy, With Template

MICHAEL GOAD,

A mobile security policy is vital to securing an organization's work environment by defining potential risk factors. But these policies are more than legal contracts, educational material and a guide to what's permitted on enterprise mobile devices.

As more cyberattacks target mobile devices, the need to refresh mobile device management (MDM) security policies is greater than ever. So, what should IT departments know about mobile policy enforcement? And what should they include if they need to refresh their existing mobile security policy?

What are mobile device security and BYOD policies?

Corporate IT policies can address several technology and usage issues for employees. IT is generally responsible for defining which security policies are necessary, but HR also plays a key role in highlighting other important technology policies. Some topics that IT policies should cover include the following:

- Internet use.
- Data retention.
- Corporate mobility.
- BYOD programs.
- Social media use.
- Change management.

The absence of a mobile security policy can lead to data breaches and other costly problems if employees aren't aware of the risks of improper use. Incidents such as sharing a patient's protected health information with unauthorized users via texts or social media are a clear violation of HIPAA rules, which can lead to serious legal and financial ramifications.

WHAT SHOULD MOBILE SECURITY AND BYOD POLICIES INCLUDE?

Mobile security and BYOD policies are gaining more attention from corporate IT due to the growing concerns surrounding smartphone use. As a result, admins must fine-tune existing corporate policies to adjust to the changing threat landscape. In general, mobile security and BYOD policies should include the following documents:

- Acceptable use policy for mobile devices.
- BYOD, choose your own device (CYOD), company-owned, personally enabled (COPE) devices and company-owned, business-only (COBO) policies.
- Mobile security policy.

In addition to these core policies, organizations can also choose to include the following:

- **Device registration form.** This form outlines the process of registering devices into management to enable access to corporate data and apps.
- **Information security.** This policy outlines the requirements for information security on devices.
- **Employee training and acknowledgment documents.** This policy outlines the training and acknowledgment documents that employees must complete.
- **Security incident response plan.** This plan outlines the step-by-step instructions for cybersecurity incidents and provides the contact information for security administrators.
- **Audits.** This policy outlines the procedures for audits that IT might conduct to ensure device compliance.
- **Enforcement.** This policy outlines the consequences of not meeting mobile security standards and the disciplinary action that admins might take in such cases.
- **Use and return of mobile devices.** This policy lays out the process for returning mobile devices upon an employee's departure, including the remote wiping and destruction of data to protect sensitive information.

Mobile device security policy best practices

Smartphones and other mobile endpoints have become an indispensable part of daily operations within any enterprise organization. As this shift blurs the line between personal and professional use, a robust mobile device security policy is imperative.

This policy safeguards an organization's data and IT infrastructure by educating end users on acceptable use and establishing management standards.

When designing and implementing mobile device security policies, admins should include best practices, such as data encryption, regular software updates and more.

ESTABLISH CLEAR POLICIES

Effective communication is vital when creating mobile security policies for both admins and end users. Be sure to establish precise guidelines that cover all relevant details and are easy for users to understand. This should encompass acceptable use, password requirements, app usage and data protection measures.

In most organizations, employees review corporate policies and documents during the onboarding process. Thus, IT must keep track of user registrations and keep the organization's mobile security policy up to date.

IMPLEMENT AUTHENTICATION AND ACCESS CONTROLS

Strict access controls such as strong passwords and biometric authentication can help reduce the risk of unauthorized access to sensitive mobile data. Furthermore, IT should use conditional access tools that ensure devices comply with specific criteria,

such as device health, OS, location and network. These tools also enforce authentication requirements such as multi-factor authentication and password policies.

ENROLL DEVICES INTO MDM

Use MDM tools to centrally enforce security policies -- including remote device wipe, configuration management and app distribution -- for all mobile devices in the organization.

ENFORCE DATA ENCRYPTION

As part of MDM, it is important to use tools that enforce encryption on all mobile endpoints in case of loss or theft.

ENABLE REMOTE WIPE CAPABILITIES

Industries such as healthcare have strict regulations to protect sensitive data. When creating mobile device policies, organizations

When creating mobile device policies, organizations must ensure that they can remotely wipe and reset devices in the event of loss, theft or an employee's departure.

must ensure that they can remotely wipe and reset devices in the event of loss, theft or an employee's departure. This helps to keep sensitive data out of the wrong hands when the device is no longer under corporate supervision.

PERFORM REGULAR UPDATES

To address known vulnerabilities and protect against emerging threats, IT must ensure that mobile devices receive regular security updates and patches. This applies to both the OS and installed apps. Organizations can centrally manage this process through MDM for company-owned devices. They can also include requirements in their policy to ensure that employees keep up with device OS updates. This will ensure device compliance and security.

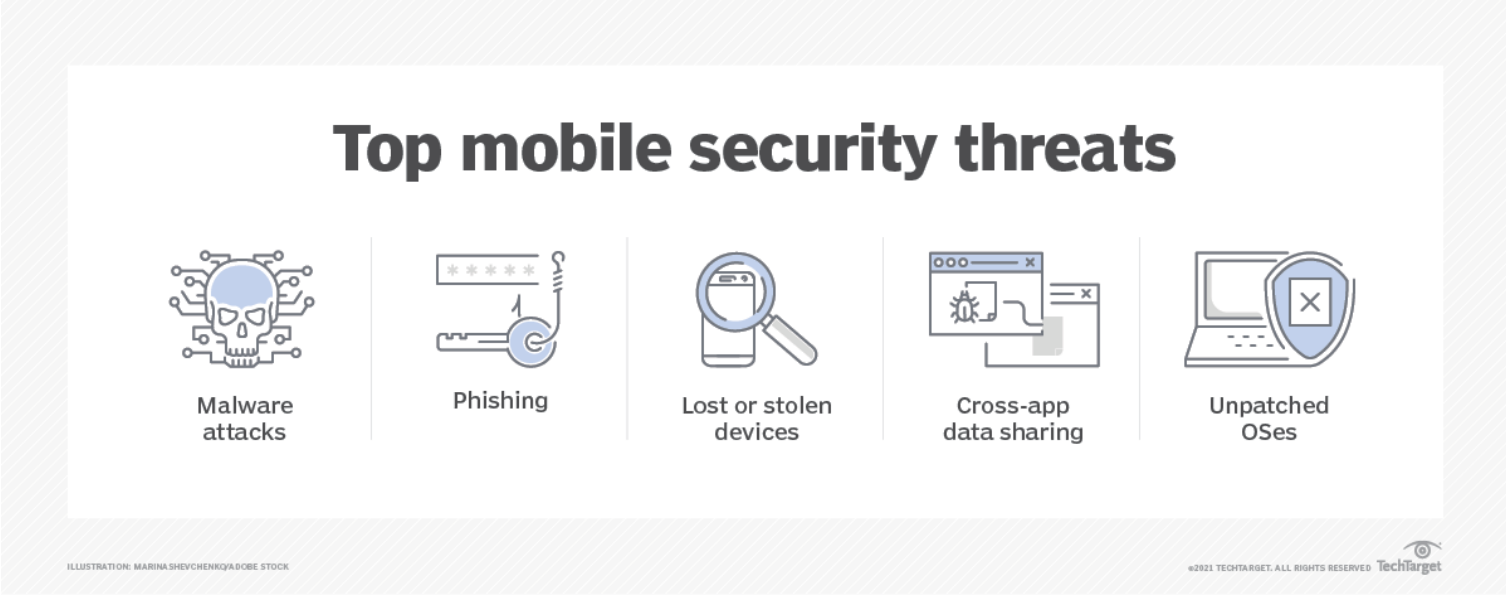
CREATE APPLICATION ALLOWLISTS AND BLOCKLISTS

In recent years, several organizations have decided to block specific apps, such as TikTok, due to data concerns. This has caused other organizations to question which apps are acceptable on a device. Organizations might not have complete control over which apps users install on devices, especially BYODs. Still, they should regularly review and develop policies to specify which apps are safe and acceptable.

PROVIDE SECURITY AWARENESS TRAINING

Training and awareness programs can help educate employees on mobile security risks and how to handle them. Many cyberattacks rely on human error, so end users need to know how to spot and respond to suspicious activity such as phishing texts and malware.

A mobile device security policy is not merely a document but an action plan for organizations. The right guidelines can ensure the safety of important data without hindering functionality for end users.



Mobile security and BYOD policy guidelines

The content of mobile security and BYOD policy documents can vary based on an organization's requirements and device security strategy. A typical mobile policy template should contain several sections which IT can edit and customize.

The first step is to clearly outline the purpose and scope of the policy. Include details of the usage of both corporate-owned and personal devices that have access to business data. Additionally, emphasize the importance of security measures and compliance requirements. Even if employees are allowed to use their personal mobile devices for work purposes, it should be mandatory to adhere to the policy, with failure to comply resulting in the revocation of this privilege. The policy must cover all devices that are capable of accessing or storing corporate data, including laptops, tablets and smartphones.

Admins can include the following sections to create a comprehensive mobile security policy. Follow the downloadable sample policy as an example of what this type of document looks like and the important guidelines to cover.

PURPOSE AND SCOPE

Highlight the purpose of the policy, what it covers and the consequences of not meeting its requirements. Broadly establish guidelines for accessing corporate data on both company-owned and personal mobile devices.

ACCEPTABLE USE

Describe the expectations employees should meet when using their devices to interact with corporate data or connect to the corporate network. This section can include the following stipulations:

- Users must always keep their apps up to date when accessing work content and resources.
- The mobile device should have basic protections such as passcodes, and users must enable encryption.
- Employees should not access websites and content deemed to be illicit, proprietary or illegal.
- Employees should not use their devices for work-related tasks during activities such as driving or operating machinery or to host and share content in the corporate network.

DEVICE RESTRICTIONS AND SECURITY REQUIREMENTS

Outline requirements concerning app management tools to ensure corporate apps and data are secure on the device. This section should address the security configurations IT must implement and the precautions that employees must take to ensure that a device interacts with corporate data. The specific details can include the following:

- Ensure that employees keep their devices up to date with the latest firmware, OS patches and antivirus protections.
- Require employees to use strong passwords on their devices with a minimum number of characters.
- Forbid employees to jailbreak or install illegal or pirated software on a mobile device used to access company data.
- Emphasize that in the event of loss, theft or any security incident involving a mobile device, employees must promptly notify the IT department.

APPROVED DEVICES AND AVAILABLE IT SUPPORT

A mobile device security policy can include a list of approved device models and operating systems. This ensures that only devices that meet compliance requirements can interact with corporate resources. Outdated and unpatched devices are more vulnerable to threats and can be difficult to manage. Whether a user accesses corporate resources on an iOS or an Android device, for example, might

also affect IT's management approach. Outside of business apps, IT generally defers to the mobile device vendor for phone support. Still, organizations should make support expectations clear to employees.

AUDITS

Detail how the organization might conduct periodic audits of devices to ensure compliance with the security policy.

USE AND RETURN OF MOBILE DEVICES

When a company provides mobile devices to its employees, it's important to keep a record of who has received the device. This policy outlines the user's responsibility to follow corporate guidelines. Measures users must take include avoiding theft or unauthorized access, enrolling the device in the company's management system and complying with all policies. When a user no longer requires the device or leaves the company, they must return all their corporate-owned mobile devices. The organization will verify that IT has properly removed all confidential information from the device before re-issuing it in accordance with the policy.

ENFORCEMENT

This policy outlines the individuals in charge of enforcing the organization's mobile policies and ensuring compliance. It also describes potential consequences of noncompliance, such as corporate data removal, device quarantine and remote wipe and reset. It should also state any disciplinary action that the organization can take against noncompliant end users.

BYOD VS. CORPORATE-OWNED ENDPOINTS

Organizations often place stricter controls on CYOD, COBO and COPE endpoints than on BYOD endpoints. Outline the ramifications of using corporate-owned devices in terms of MDM, restrictions on content access and employee liability in the case of device damage.

Editor's note: *This article was originally published in 2021 and was updated in 2024 to improve the reader experience.*

Michael Goad is a freelance writer and solutions architect with experience handling mobility in an enterprise setting.

In this handbook:

How to Create a Mobile Device Security Policy, With Template

Reda Chouffani runs the consulting practice he co-founded, Biz Technology Solutions, Inc. He is a healthcare informatics consultant, cloud expert and business intelligence architect who helps enterprise clients make the best use of technology to streamline operations and improve productivity.