**ACME Secure Mobile Computing Policy**

**Using this policy**

One of the challenges facing IT departments today is securing both privately owned and corporate mobile devices, such as smartphones and laptops. This example policy is intended to act as a guideline for organizations looking to implement or update their mobile device security policy.

Feel free to adapt this policy to suit your organization. Where required, adjust, remove or add information according to your needs and your attitude towards risk. This is not a comprehensive policy, but rather a pragmatic template intended to serve as the basis for your own policy.

**Background to this policy**

The most common challenge to organizations is that users do not recognize that mobile devices represent a threat to IT and data security. As a result, they often do not apply the same security and data protection guidelines as they would on other devices, such as desktop computers.

The second challenge is that when users provide their own devices, they often give greater weight to their own rights on the device than to their employers' need to protect data.

This outline policy gives a framework for securing mobile devices and should be linked to other policies that support your organization's posture on IT and data security.

Mobile Security Policy

1. **Objective**

ACME Retail is an American department store chain with over 1,000 retail brick and mortar stores that sell household goods to the consumer market. ACME Retail also has an online e-commerce storefront with a corresponding mobile application for consumers to order household goods from their mobile devices. The purpose of this document is to outline a high-level mission for our security strategy that encompasses the following components of our business: **Mobile Infrastructure, Mobile Communications, Mobile Devices, Mobile Platforms, Mobile Applications, and Mobile Cloud Computing.**

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However, mobile devices also represent a significant risk to information security and data security; if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization’s data and IT infrastructure. This can subsequently lead to data leakage and system infection.

ACME Retail has a requirement to protect its information assets in order to safeguard its customers, intellectual property, and reputation. Specifically, since the organization accepts credit/debit cards for purchase, it is required to comply with The Payment Card Industry Data Security Standard (PCI DSS). This document outlines a set of practices and requirements for the safe use of mobile devices.

1. **Scope**
2. All mobile devices, whether owned by ACME Retail or owned by employees, that have access to corporate networks, data, and systems, not including corporate IT-managed laptops (this includes smartphones and tablet computers)
3. Mobile Infrastructure: The mobile infrastructure consists of an enterprise WLAN with 50 access points implemented across 5 buildings.
4. Mobile Communications: The mobile infrastructure uses 802.11 communications.
5. Mobile Devices: Company official-use android devices are issued and employees use personal devices to access email and enterprise applications with mobile device management implemented.
6. Mobile Platforms: ACME-issued mobile devices implement the Android platform.
7. Mobile Applications: ACMEApp is the production application that is implemented on the customers' mobile devices and is available on Google Play and the iPhone App Store.
8. Mobile Cloud Computing: ACMEApp leverages Cloud Computing to process, transmit, and store data.
9. Exemptions: If there is a business need to be exempted from this policy (e.g., too costly, too complex, adversely impacting other business requirements), a risk assessment must be conducted after being authorized by security management.
10. **Mobile Device Policy**
    1. Technical Requirements
11. Devices must use the following Operating Systems: Android 10x or later, iOS 12x or later.
12. Device must have remote data wipe functionality enabled.
13. Data deletion must occur after 10 unsuccessful password attempts.
14. Devices must store all user-saved passwords in an encrypted password store.
15. Devices must be configured with a secure password that complies with ACME Retail’s password policy. This password must not be the same as any other credentials used within the organization.
16. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.  
    1. User Requirements
17. Users must only load data essential to their role onto their mobile device(s).
18. Users must report all lost or stolen devices to ACME Retail IT immediately.
19. If a user suspects that unauthorized access to company data has taken place via a mobile device, the user must report the incident in alignment with ACME Retail’s incident handling process.
20. Devices must not be “jailbroken”\* or have any software/firmware installed that is designed to gain access to functionality not intended to be exposed to the user.
21. Users must not load pirated software or illegal content onto their devices.
22. Applications must only be installed from official platform-owner-approved sources. Installation of code from untrusted sources is forbidden. If you are unsure whether an application is from an approved source, contact ACME Retail IT.
23. Devices must be kept up-to-date with manufacturer or network-provided patches. At a minimum, patches should be checked for weekly and applied at least once a month.
24. Devices must not be connected to a PC that does not have up-to-date or disabled anti-malware protection and does not comply with corporate policy.
25. Devices must be encrypted in line with ACME Retail’s compliance standards.
26. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify ACME Retail IT immediately.
27. Users must not use corporate workstations to backup or synchronize device content, e.g., media files, unless such content is required for legitimate business purposes.
28. Users must be capable of identifying phising attacks and delete suspicious emails immediately.

\*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all of its features and enabling the installation of unauthorized software.

* 1. Mobile Infrastructure Policy

1. Inventory of Authorized and Unauthorized Devices: All authorized and unauthorized devices (Bring Your Own Device or Corporate) will have unique IDs that will be stored in a secured database.
2. Software Security: Application Software Security is implemented to manage the security lifecycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.
3. Physical Security: All 5 buildings must use corporate badging and proper identification techniques to protect access to critical network infrastructure.
   1. Mobile Communications Policy
4. Data Encryption: All data that is transferred over the mobile communications network or at rest on the network must be encrypted.
5. Network Identifier Refreshing: Radio Network Temporary Identifiers (RNTI) must be refreshed whenever a user device connects to the corporate network.
6. LTE Fallback Prevention: Ensure that LTE fallback−a known security risk−is disabled both at the carrier and user levels.
   1. Mobile Platform Policy
7. Device Patching: All ACME-issued Android devices are patched regularly with the latest Android release to prevent malware and data leakage.
8. Unknown Sources: Users are educated on the dangers of playing audio/video files from unknown sources.
9. Permission Restrictions: Users must never install an application that seeks full permission to access everything on the device.
10. Platform Security: All system components have restricted access and strict access policies.
    1. Mobile Application Policy
11. Source Code Obfuscation: All source code related to ACMEApp is to be obfuscated to prevent reverse engineering.
12. Secure Data Storage: ACMEApp payment system will store all data on the cloud and never on the device itself to prevent data theft.
13. Secure Data Storage: Access to cardholder data is restricted greatly and only enabled for business purposes.
14. Transport Layer Protection: ACMEApp will use HTTPS exclusively and data encryption to ensure the safe delivery of sensitive data.
15. Bug Detection and Prevention: ACMEApp is tested regularly to identify bugs and ensure proper security settings.
    1. Mobile Cloud Computing Policy
16. Backend-as-a-Service (BaaS) Implementation: ACMEApp developers will seek out high-level documentation to ensure the proper security guidelines are noted during implementation.
17. Root Key Access: ACMEApp developers will never give users root key access and ACMEApp will display a warning notification if this occurs.
18. Developer Responsibility: ACMEApp developers will be given a detailed outline of data security laws and regulations annually and will be required to adhere to these policies during all phases of application development.