Sam Mendez

Mobile Device Security Policy

(Hipster Version)

**1. Introduction**

Welcome to SAM Worldwide, where mobility meets security. In our fast-paced world, smartphones and tablets are the engines that drive productivity, but with great mobility comes great responsibility. Our Mobile Service Security Policy serves as the guiding force to ensure that the pulse of our organization remains secure and protected.

At SAM Worldwide, we recognize the key role that mobile devices play in our daily operations. Whether owned by the company or our valued employees, these devices are powerful tools that demand a vigilant approach to security. This policy outlines the superhero code for safeguarding our data, ensuring that the information that fuels our success remains resilient against potential threats.

Join us on this journey where technology meets security, and together, let's support the mobile landscape of SAM Worldwide. It's not just a policy; it's our commitment to maintaining the confidentiality, integrity, and availability of our information in the ever-evolving realm of mobile services.

2. **Purpose**

2.1. This rule covers all mobile devices, whether the organization owns them or they belong to our cool employees. Laptops managed by IT are the VIPs who get a pass. If we need an exception, we have to prove it's worth it through a risk assessment.

3. **Policy**

3.1. **Tech Stuff**

3.1.1. Our devices need to run on Android 6.2 or newer, or iOS 9.6 or newer. No old-school stuff here.

3.1.2. Passwords we save on our devices? Keep 'em in a secret, encrypted vault.

3.1.3. Lock your device with a strong password that's different from any other secret codes you use in the organization.

3.1.4. Unless IT is babysitting, our devices can't plug directly into the super-secret corporate network.

3.2. **User Life**

3.2.1. Only save the important work stuff on your device. No funny business.

3.2.2. If you lose your device, tell the IT squad ASAP.

3.2.3. If you smell something fishy with your device and think someone's messing with our company data, report it like a true hero.

3.2.4. Don't mess with jailbreaking or installing shady software. It's a no-go.

3.2.5. No pirated software or illegal stuff on our devices. Keep it clean.

3.2.6. Only download apps from the legit app stores. If in doubt, hit up the IT crew.

3.2.7. Keep your device updated with patches. Check weekly and update at least once a month.

3.2.8. Don't connect your device to a sketchy computer. Make sure it's armed with anti-malware protection and follows our company rules.

3.2.9. Encrypt your device, following our company's rules. Keep it secret, keep it safe.

3.2.10. Be careful mixing personal and work emails. Only send company stuff through our work email.

3.2.11. If you're backing up or syncing stuff, do it on work computers only if it's legit for business.

3.3. **Device Management and Monitoring**

3.3.1. We're getting some extra eyes on our devices. IT superheroes will install mobile device management (MDM) software on company-owned devices for remote tracking, management, and wiping if they decide to go on a solo mission (get lost or stolen).

3.3.2. Make sure your device is on the radar by registering it with the IT department. We're keeping tabs on all our superhero gadgets.

3.4. **Data Encryption and Storage**

3.4.1. Encrypt your device - it's like having a secret code to protect our data. Make sure this is set up; it's not negotiable.

3.4.2. Avoid storing top-secret data on your device. If possible, use secure cloud storage or our company servers. Keep our secrets safe and sound.

3.5. **Authentication and Access Controls**

3.5.1. Keep things in check by reviewing and updating who gets access to what. Adjust permissions based on who needs them - not everyone gets the keys to the kingdom.

3.6. **Network Security** 3.6.1. When connecting to public Wi-Fi, cloak up with a virtual private network (VPN). We're not exposing ourselves on unsecured networks or open Wi-Fi connections.

3.7. **Incident Response**

3.7.1. If something smells phishy or looks suspicious, report it pronto. We've got an incident response plan for dealing with these situations. Be a hero and report any weird behavior.

3.7.2. Don't keep security breaches to yourself. If you spot trouble, shout it out to the IT department. They're our crisis avengers.

3.8. **Device Disposal**

3.8.1. When it's time to part ways with your device, follow the rules for wiping data. We don't want our secrets falling into the wrong hands.

3.8.2. Hand over retired devices to the IT department for proper disposal and recycling. Let's make sure our old gadgets rest in peace.

3.9. **Training and Awareness**

3.9.1. Join our superhero training sessions on mobile security. We're keeping everyone in the loop on the latest threats and how to stay vigilant.

3.9.2. If you see something strange, say something. We're all part of the security squad, and every hero plays a role.

3.10. **Legal and Compliance**

3.10.1. Stick to the rules. Our mobile device use should comply with the law. We're not breaking any superhero codes here.

3.10.2. Stay informed about legal requirements. We'll update the policy when the law updates its rules.

3.11. **Periodic Audits**

3.11.1. The auditors are coming! We'll be doing surprise checks on devices to make sure everyone's following the superhero guide. Non-compliance might mean losing some gadget privileges.

3.12. **App Permissions and Reviews**

3.12.1. Keep an eye on app permissions. We're not giving away more than we should. Report any apps acting suspiciously - we're the detectives here.

3.12.2. If you're not sure about an app, check in with the IT crew. They're our app guardians.

3.13. **Device Tracking and Geolocation Services**

3.13.1. Activate tracking and geolocation. It's like having a GPS for your device. Only enable location services when you need them - no one needs to know your every move.

3.14. **Biometric Authentication**

3.14.1. Use your fingerprint or face for an extra layer of security. But keep that biometric data to yourself - we're not sharing it with random apps.

3.15. **Remote Wiping and Locking**

3.15.1. If your device goes MIA, we've got the power to wipe it remotely. Test it out - make sure it works when we need it.

3.16. **Social Engineering Awareness**

3.16.1. Be on the lookout for tricksters. Don't spill any secrets, even if someone sounds legit. Report anything fishy - we're not falling for any mind games.

***Part 2***

**Why is it important for organization to use Security Engineering process?**

Security engineering processes are crucial for risk mitigation, compliance, protection of assets, maintaining trust, and adapting to evolving threats.

**Name the Five Phases of the Engineering Lifecycle used in NIST SP800-27:**

1. Initiation Phase
2. Development/Acquisition Phase
3. Implementation Phase
4. Operation/Maintenance Phase
5. Disposition Phase

**Which part of the Security Engineering process is the most important and why?**

The Initiation Phase is the most important because it involves strategic decision-making, establishing security requirements, conducting initial risk assessments, and allocating resources for a secure system development. These decisions set the foundation for the entire lifecycle.Top of Form

References:

Guerin, N. (2022, January 18). *Security Policy for the Use of Handheld Devices in Corporate Environments*. SANS Institute. https://www.sans.org/white-papers/32823/

Wayne County Community College District. (n.d.). Mobile Device Acceptable Use Policy. https://www.wcccd.edu/dept/pdf/IT/mobile\_policy.pdf