Remote device security policy template

Why do organizations need remote device security?

Organizations rely on remote devices, such as laptops, smartphones, and tablets, to keep their operations running smoothly. These remote devices offer the flexibility for employees to work from anywhere, which has become especially important in today's digital age. However, this flexibility comes at a cost that includes the security risks associated with remote devices.

Implementing a comprehensive remote device security policy is critical for any organization that wants to protect its assets and maintain the integrity of its data. A remote device security policy sets out guidelines for using remote devices safely and securely. It includes a range of measures that organizations can take to minimize the risks associated with remote devices. By implementing this policy, organizations can also ensure that their employees are taking appropriate measures to protect sensitive information and minimize the risk of security breaches.

In addition, by using a UEM solution, organizations can simplify the management of remote devices and improve their security posture. A UEM solution provides IT admins with the tools they need to ensure that remote devices are secure and up to date. It can automate several repetitive tasks, freeing up IT resources to focus on other critical tasks. With a UEM solution, organizations can ensure that their remote devices are suitably protected from security risks and other threats.

Table of Contents

<Company>: remote device security policy

1. Introduction

<Company> remote device security policy outlines the requirements and guidelines for securing remote devices used in the <Company>. The purpose of this policy is to establish security measures to protect sensitive data and systems from potential security breaches, unauthorized access, or other security threats. This policy applies to all remote devices owned, authorized, or issued by the <Company>, and to all employees who use remote devices to access the <Company>'s systems and data.

2. Scope

This policy applies to all employees of <Company> who use remote devices to access company information systems and data, whether they are owned by the company or personally owned by the employee.

3. Policy

3.1 Acceptable Device Usage

Employees will be allowed to use corporate-owned or personal devices for work. All the employees must enroll their devices used for work in the UEM solution authorized by <Company>.

The devices must be regularly and periodically monitored via the UEM solution to ensure compliance with policy requirements.

Employees are responsible for the complete ownership of their respective devices and must report any loss or damage to them. They should also sign a <User agreement> before connecting their respective mobile devices to the authorized organization network.

All devices must be encrypted using the UEM solution to ensure security and to protect company data and resources. Any issues with devices must be reported to the help desk of the <Company>.

To ensure secure remote device usage, it is strictly prohibited to download any unauthorized software onto the device without the permission of the <IT team>. Additionally, all users must take necessary precautions to avoid leaving their devices unattended in public spaces to prevent potential security breaches or physical loss of the device.

3.2 Password security

To ensure a secure environment, all devices must be password-protected using strong, unique passwords that adhere to <Company> 's password policy. Users should update their passwords every <days/months>.

To reduce the risk of data breaches, it is recommended that sensitive information be stored on the device for a minimum of <days/months> only, to ensure proper record-keeping and safe removal of outdated data. Users must never disclose their passwords to anyone, including coworkers, family, or friends.

All devices should comply with the password policy pushed by the UEM solution. This policy may include requirements for password length, complexity, and many more.

3.3 Personal device usage

The <Company> supports a BYOD policy that requires end users to register their devices with the <IT team> for authorization. All sensitive information and resources related to <Company> should be stored separately and encrypted on personal devices. The use of the <Company> network and email system for personal purposes is not allowed.

3.4 Network management

To ensure the security of the network and data of <Company>, only mobile devices that support SSL and VPN are allowed to access them. This VPN configuration must be set up using a UEM solution.

The end user must ensure that their device is connected to a secure Wi-Fi network, and when working remotely, only authorized networks should be connected. To maintain data protection and device security, further configurations on VPN and APN settings must be enabled.

End users must follow the established security measures and adhere to all rules and regulations issued by <Company>. When the end user software isn't working correctly, they should notify the appropriate <IT team> immediately to avoid any information security risks.

The <IT team> is responsible for managing all company-managed devices and keeping them up to date by distributing necessary updates and patches using a UEM solution.

Personal devices provided by <Company> are strictly used for work purposes only, and the end users should avoid making personal use of them. The end user is responsible for keeping anti-virus and anti-malware software up to date to ensure that the device is adequately protected.

3.5 App usage

Approved applications installed by <Company> must always be available on managed devices and should not be removed.

Employees cannot install or use personal apps on <Company> mobile devices, but they may recommend an app for job-related tasks. The corresponding department will handle the request after discussing it with the <IT team>.

<Company> will use the UEM solution to enforce a blacklist policy for all applications unrelated to business activities.

Whitelisted apps approved by <Company> via the UEM solution will only be permitted for use in kiosk mode. Employees may use a browser whitelisted by <Company> or the dedicated kiosk browser provided by the UEM solution, and all other browser use is strongly discouraged.

Periodic checks by the <IT team> should ensure the necessary applications are up to date on the remote devices. Mandatory applications supporting various business activities and ensuring smooth daily operations at <Company> will be classified through the UEM solution.

Employees should not alter any app configurations or settings defined by <Company>. The <IT team> is responsible for pre-defining app configurations and permissions during device enrollment.

3.6 Content management

Under no circumstances should employees upload personal files onto <Company> remote devices. Employees must ensure that confidential files and resources of <Company> on their remote devices are backed up correctly.

The <IT team> will periodically check the devices to ensure that they only contain files authorized by <Company>. Downloading videos, music, games, or other software on remote devices for non-work purposes is strictly prohibited.

Employees are strictly prohibited from downloading or sharing sensitive information of <Company> to personal devices or third parties. Restrictions on several file-sharing functions, such as Bluetooth, USB file transfer, OTA file transfer, and NFC, will be enabled via the UEM solution to reduce the risks associated with unauthorized access.

3.7 Remote wiping of device

The UEM solution can remotely wipe all data from a device if it is lost or stolen.

The <IT team> may initiate a remote wipe of the device in the event of a security breach or violation of the acceptable usage policy.

The end-users are responsible for backing up any personal data before a remote wipe is performed. The devices must be regularly and periodically monitored via the UEM solution and encrypted to protect the data and resources stored on them.

All end users are required to comply with these procedures to maintain the security of the <Company> 's information systems.

3.8 Report lost or stolen devices

In case a device is lost or stolen, the end user should immediately report it to the <IT team> and <concerned manager>. The report must include the details of the device such as make, model, and serial number.

The <IT team> will then take the necessary actions to ensure the device and its data are secured. This may include remotely wiping the device to prevent any unauthorized access.

End users are also advised to take precautionary measures to protect their devices from loss or theft, such as not leaving devices unattended in public places and using secure carrying cases for transportation.

It is the responsibility of the end user to keep the <IT team> informed of any changes in device ownership or location. Failure to report a lost or stolen device in a timely manner may result in disciplinary action and potential legal consequences.

3.9 Remote monitoring and management

To ensure that the company's remote devices are being used properly and to their full potential, remote monitoring and management will be implemented by the <IT team>. This includes monitoring the security of the device, as well as ensuring that employees are not engaging in improper usage of the device as outlining in section 3.10.

Remote management also enables the <IT team> to push software updates, patches, and other necessary changes to the devices.

Additionally, remote monitoring can detect and report on any issues that may affect device functionality or workflow, allowing for swift resolution by the concerned manager.

All the employees are expected to cooperate with remote monitoring and management measures, as this will help ensure the integrity and security of the company's data and resources.

3.10 Location tracking of remote devices

Remote devices may be subject to location tracking to ensure the security and safety of <Company> resources. This tracking will only be used for authorized purposes, such as locating a lost or stolen device or ensuring employee safety during business travel.

Employees will be notified of the location tracking policy and the purpose of the tracking. The tracking data data collected will be kept secure and confidential, accessible only to authorized personnel of <Company> for approved purposes.

If an employee has concerns about location tracking, they should contact their manager or the IT team to discuss their options. The company will work to accommodate reasonable requests to the best of its ability.

Employees are expected to keep their remote devices charged and with them at all times when traveling for business purposes to ensure accurate location tracking. If an employee is unable to carry their device, they must inform their _____<concerned manager>_____ and obtain approval for alternative tracking methods.

Location tracking will only be used in compliance with applicable laws and regulations and will not be used to monitor personal activities or outside of authorized purposes.

3.11 Improper usage of remote devices

Employees are strictly prohibited from downloading, installing, or using any software that could compromise the security of _____<Company>_____'s resources and data. This includes any software that could enable third parties to identify and exploit vulnerabilities in remote devices.

In case employees notice any issues that could affect the functionality of the device and workflow, they should notify their concerned manager immediately. Inappropriate use of mobile devices includes, but is not limited to, the following:

- Removing mobile devices from UEM enrollment without obtaining permission from _____<Company>_____.
- Anything that puts the confidentiality and accessibility of business and client data at risk.
- Unauthorized personal use of mobile devices.
- Intentional damage to mobile devices.
- Allowing non-employees to access _____<Company>_____ data.

3.12 Breach of policy

Any intentional or unintentional violation of this policy or its provisions will result in disciplinary action by _____<Company>_____. Employee who breaches this policy may have their work privileges terminated by management.

<Company>: remote device security policy

1. Employee details:

Name: <Name of the employee>

Employee ID: <Employee ID>

Department: <Employee department>

Manager: <Name of the manager>

2. Work details:

Address: <Address of the employee>

Phone number: <Phone number of the employee>

All of the conditions and expectations outlined in the policy have been read, I completely comprehend them, and I accept them.

Employee: <Signature of the employee>

Manager: <Signature of the manager>