

Rugged Device Usage Policy Template

Why do you need a rugged device usage policy?

Rugged devices are hardware specially designed to withstand and operate under the harshest of environmental conditions. They are built with specifications to far exceed that of consumer and other commercial grade devices.

Their ruggedness is determined based on the outcomes of multiple tests such as MIL-STD tests and the Ingress Protection (IP) scale. While Windows and Android are some of the most used operating systems, businesses may slowly have to incorporate more devices running on Android, as Microsoft is well on its way to limit the support of Windows Embedded CE 6.0 and Windows Embedded handheld devices.

Rugged devices are used by a wide range of industries, some of which includes Construction, Military, Logistics, Healthcare, Retail and Manufacturing. Since these devices are often used outdoors, they can be a constant worry for organizations, as they would have to continually monitor device security, data protection and ensure it stays connected to secure networks. A Unified Endpoint Management (UEM) solution can provide your IT team with all the controls they need to get this easily done. Integrations with Android Enterprise and support for OEMConfig can smoothen out multiple challenges admins often encounter while managing the rugged devices.

Implementing a rugged device usage policy can help organizations implement security measures of their own and educate employees on the proper usage of these devices.

Table of Contents

Introduction.....	3
Scope.....	3
Policy.....	3
Technical Requirements.....	3
Acceptable Use.....	3
Device Security.....	4
Application Security.....	4
Network Security.....	5
Content Management.....	6
Requirements of devices taken off-site.....	6
Lost or stolen devices.....	6
Improper usage of devices.....	7
Breach of Policy.....	7

_____ : Rugged Device Usage Policy

1. Introduction

This policy defines the set of practices and guidelines employees should follow with respect to the safe usage of rugged devices managed by _____ and sensitive information present within the devices.

2. Scope

All rugged devices and applications, managed and owned by _____, that can have access to _____'s networks, data and other systems.

3. Policy

3.1. Technical Requirements

3.2. Acceptable Use

All employees should comply with _____'s policy when using the rugged devices. If employees are not sure of their responsibilities regarding the usage of the devices, they can reach out to _____ to get it clarified.

Employees should not download, install or run any programs or utilities that could lead unauthorized external parties to spot and exploit any weaknesses within the rugged devices.

3.3. Device Security

The rugged devices should comply with _____'s password policy. The policy shall be remotely pushed via a UEM solution.

Passwords used in applications and other websites should be stored in a password manager. A strict clear screen and clear desk policy should be maintained within _____'s premises.

Various restrictions shall be placed on the device functionality and other settings to ensure they continue to function in alignment with the usage policies set by _____ and to dissuade users from sharing sensitive information.

_____ should make sure all employees within their respective teams have the latest operating system installed within the rugged devices. This is done to ensure device protection and to minimize the possibility of any risks pertaining to unauthorized access and data leakage.

The devices shall be encrypted via a UEM solution to ensure data protection.

It is the responsibility of all employees to ensure data stored within the device are backed up at regular intervals.

The devices shall be subjected to periodic compliance checks to ensure they stay compliant with the policies defined by _____.

3.4. Application Security

Employees are strictly forbidden to install, download and run applications for personal use. Employees can, however, suggest the use of an application for work related purposes. This should be sent in as a request to the _____ team, who will then process the request by consulting with the _____ or other members of the _____.

The applications shall be installed via a UEM solution to ensure they are installed only from approved sources. These shall be updated whenever a new version is available.

Users shall be restricted from making any changes to the app configurations or settings to ensure data integrity. App configurations and permissions shall be pre-defined by the _____ during the device enrolment process.

_____ shall maintain a policy of blacklisting applications deemed irrelevant to its business operations. Rugged devices operating in kiosk mode shall only run whitelisted applications that has been previously approved by the _____.

Employees could either use the dedicated kiosk browser offered by the UEM solution or use a browser whitelisted by _____. Use of any other browsers are strictly discouraged.

3.5. Network Security

Email settings shall be configured and data loss prevention policies shall be remotely enabled on the devices to protect the corporate and client confidential information. All employees are expected to comply with the various technical and operational measures taken up by _____ with respect to email security to safeguard the information they work with.

If employees suspect they have been subjects to a phishing scam or are the recipients of a malicious mail, they must immediately report it to the _____. Other instances of malware attacks and identity thefts should be promptly reported to the _____ as well.

Web filtering shall be enabled on the devices solely for the purpose of improving employee productivity and restricting employees from connecting to websites prone to malicious content, scams, malware attacks and other cybersecurity threats.

Employees can reach out to their concerned _____ or any members of the _____ to fully understand the web filtering policies of _____.

3.6. Content Management

Employees are strictly forbidden from uploading any personal files onto the devices. The _____ shall monitor the devices on a periodic basis to ensure they only consists of files approved by the organization.

In order to curb any risks related to unauthorized access, restrictions on various file sharing functionalities such as Bluetooth, USB file transfer, OTA file transfer and NFC shall be enabled.

Access to corporate emails and other content shall be managed via a UEM solution.

3.7. Requirements of devices taken off-site

When working remotely, employees should only connect their devices to a network that has been approved by _____. Further configurations on the VPN and APN settings shall be enabled to monitor and ensure data protection and device security.

Employees are responsible to ensure the safety of their own devices. They should not be left unattended in public places. Avoid sitting in crowded places to limit the chances of unauthorized access to sensitive data through shoulder surfing.

A clear desk and clear screen policy should be maintained off-site.

3.8. Lost or stolen devices

If a device is lost or stolen, employees should immediately report it to their _____. The _____ would then remotely lock the device and wipe its data from the UEM console.

Various other remote actions shall be enabled to ensure the lost device stays completely protected.

3.9. Improper usage of devices

If employees observe the occurrence of any incidents that could affect the functioning of the device and disruption of workflow, they should promptly report it to their concerned _____ and a member of _____. These include, but not limited to the following:

- Any incident that could compromise the availability and integrity of company and client confidential data.
- Unauthorized usage of the device i.e., using it for personal use.
- Damaging the device on purpose
- Taking the rugged devices off-site without _____'s approval.
- Allowing non-employees to access data stored within the device

3.10. Breach of Policy

Employees who wilfully disregard the requirements stated within the policy shall be subjected to disciplinary action. This will include a formal meeting with their _____ who would examine the severity of the breach and make a report based on which further actions shall be taken.