Cybersecurity Policy Templates

Mobile Device Management Policy

(Last Updated April 2025)

Purpose

Our Mobile Device Policy aims to establish a comprehensive framework for the secure and responsible use of mobile devices within our organization, including smartphones, tablets, and laptops. This policy aims to protect sensitive data, maintain the integrity of our systems, and mitigate the risks associated with mobile device usage. By implementing effective controls and practices, this policy defines acceptable use policies, enforces device security configurations, and ensures data protection measures, such as encryption and remote wiping capabilities. We strive to minimize the potential risks of unauthorized access, data breaches, and malware infections by enforcing strong authentication mechanisms, regular security updates, and employee training. By prioritizing the secure use of mobile devices, we protect the confidentiality, integrity, and availability of our information assets, maintain compliance with industry standards and regulatory requirements, and uphold the trust and confidence of our stakeholders.

Scope

The Mobile Device Policy applies to all our organization's employees, contractors, and stakeholders. It encompasses the secure and responsible use of mobile devices in work-related activities, including smartphones, tablets, and laptops. This policy covers both organization-owned devices and personal devices used for work purposes. It sets guidelines for device configuration, data encryption, authentication mechanisms, and application management to protect sensitive information and prevent unauthorized access. The policy defines procedures for mobile device registration, device monitoring, and enforcing security controls, such as remote wipe capabilities and mobile device management (MDM) solutions. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for mobile device management and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

MDM-01	Maintain a Mobile Device Management (MDM) system to enforce cybersecurity safeguards on each organization's mobile device (such as phones and tablets).
MDM-02	Ensure the organization's Mobile Device Management (MDM) system limits enterprise data on mobile devices to containerized, enterprise-managed applications.
MDM-03	Ensure the organization's Mobile Device Management (MDM) system enforces approved configurations on each of the organization's approved enterprise applications.
MDM-04	Ensure the organization's Mobile Device Management (MDM) system enforces application control on the organization's managed mobile devices, only allowing authorized applications (including mobile application stores) to execute on the devices.
MDM-05	Ensure the organization's Mobile Device Management (MDM) system enforces an unlock code to access each of the organization's mobile devices (6 characters or longer).
MDM-06	Ensure the organization's Mobile Device Management (MDM) system enforces mobile operating system updates on each of the organization's mobile devices.
MDM-07	Ensure the organization's Mobile Device Management (MDM) system enforces application updates on each mobile device.
MDM-08	Ensure the organization's Mobile Device Management (MDM) system detects and blocks jailbroken mobile devices.
MDM-09	Ensure the organization's Mobile Device Management (MDM) system can remotely wipe data from its mobile devices if they are lost or stolen.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.