US Solutions Pvt Ltd. - Mobile Device Management (MDM) Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-02-09
- **Author:** IT & Infosec Department - Marcus Flores
- **Approved By:** Annette Reynolds, IT Infrastructure Director
- **Effective Date:** 2024-03-08
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes the increasing use of mobile devices for business purposes and the associated security risks. This Mobile Device Management (MDM) Policy outlines the guidelines and requirements for managing and securing mobile devices used to access Company resources. This policy aims to protect Company data and systems while ensuring the productivity of our employees. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a framework for managing and securing mobile devices.
- Protect Company data from unauthorized access, loss, or theft.
- Ensure compliance with applicable laws and regulations.
- Define the responsibilities of Users and the IT department regarding MDM.
- Provide a secure and efficient environment for mobile device usage.

3. Scope

This policy applies to all mobile devices (smartphones, tablets, laptops) used to access Company resources, including:

- Company-owned devices.
- Personal devices used for business purposes (BYOD).
- Devices used to access Company email, applications, and data.
- Devices connected to the Company network.

4. MDM Requirements

- **MDM Software:**
    - The Company will utilize approved MDM software to manage and secure mobile devices.
    - Users are required to install and maintain the MDM software on their devices.
    - MDM software may include features such as remote wiping, passcode enforcement, application management, and location tracking.

- **Device Eligibility:**
    - Devices must meet minimum operating system and hardware requirements.
    - The IT department maintains a list of supported devices and operating systems.
    - Devices must be compatible with the Company's MDM software.
- **Security Requirements:**
    - Devices must have a strong passcode or biometric authentication enabled.
    - Devices must have up-to-date operating systems and security patches.
    - Devices must have antivirus and anti-malware software installed (if applicable).
    - Devices must have full disk encryption enabled (if applicable).
- **Application Management:**
    - Users must use Company-approved applications to access Company resources.
    - The Company may restrict the installation of unauthorized applications.
    - Company applications will be managed and updated through the MDM platform.

5. User Responsibilities

- **MDM Compliance:** Users must comply with all MDM requirements and guidelines.
- **Device Security:** Users are responsible for maintaining the physical and logical security of their devices.
- **Data Protection:** Users must protect Company data stored on their devices from unauthorized access, loss, or theft.
- **Reporting Incidents:** Users must immediately report any security incidents, such as lost or stolen devices or suspected data breaches, to the IT department ([email address removed]).
- **Acceptable Use:** Users must use their devices in accordance with the Company's Acceptable Use Policy.
- **Data Separation:** Users must make reasonable effort to keep company data separate from personal data.

6. Company Responsibilities

- **MDM Implementation:** The Company will implement and maintain the MDM platform.
- **Technical Support:** The IT department will provide technical support for MDM-related issues.
- **Policy Enforcement:** The Company will enforce this MDM Policy and take appropriate disciplinary action for violations.
- **Data Wiping:** The Company reserves the right to remotely wipe Company data from a device in the event of a security incident, termination of employment, or policy violation.
- **Privacy:** The Company will respect user privacy and will only use MDM to manage Company data.
- **Providing Secure Tools:** The company will provide secure tools and applications for use on mobile devices.

7. Data Access and Security

- **VPN Access:** Users must use a Company-provided VPN to access Company resources over unsecured networks.
- **Data Encryption:** Company data stored on mobile devices must be encrypted.
- **Access Control:** Access to Company resources will be controlled through the MDM platform and Company access control policies.

8. Legal and Regulatory Compliance

- **Data Privacy:** Users must comply with all applicable data privacy laws and regulations (e.g., GDPR, CCPA).
- **Intellectual Property:** Users must respect the Company's intellectual property rights.
- **Legal Holds:** The Company may require access to user devices for legal or regulatory purposes.

9. Termination of Employment

- **Data Removal:** Upon termination of employment, Users must remove all Company data from their devices.
- **MDM Removal:** The IT department will remove MDM software from user devices.
- **Device Return:** Any Company-owned devices must be returned to the IT department.

10. Policy Review and Updates

- This MDM Policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

11. Acknowledgement

- By using mobile devices to access Company resources, Users acknowledge that they have read, understood, and agree to comply with this MDM Policy.

This MDM Policy is designed to protect US Solutions Pvt Ltd.'s data and systems while ensuring the productivity of our mobile workforce. By adhering to these guidelines, Users contribute to a secure and efficient work environment.