Langslide

BYOD (Bring Your Own Device) Policy

Version 1.0

PURPOSE

This policy defines the rules for BYOD—Bring Your Device—and governs how employees, contractors, and other authorized end users can use personal laptops, smartphones, tablets, and other personal devices on the Rudramsa Systems Pvt. Ltd. (hereby referred to as the organization)network to access data and perform job duties. It aims to protect the security and integrity of the organization's infrastructure while enabling personnel to work efficiently.

SCOPE

This policy applies to all employees and contractors within the organization. It should be read with the Acceptable Usage Policy & Procedure and other information security-related policies.

DEFINITION

Following is an explanation of various terms used within this document:-

- **BYOD (Bring Your Device):** Personally owned devices are used to connect to the organization's network and access business data or systems.
- **Rooted Device (Android):** A device on which the user has unlocked or "rooted" the operating system, removing built-in manufacturer limitations and potentially creating security risks.
- **Jailbroken Device (iOS):** A device on which the default operating system restrictions have been bypassed to install software not approved by or available from the official App Store.
- **Registered Device:** A personal device approved and recorded by the organization for accessing secured resources (e.g., files, applications), possibly under conditional access and specific security policies.
- **Corporate Data:** Any information—such as documents, email content, credentials, or intellectual property—owned or managed by the organization, whether stored, transmitted, or processed on corporate or personal devices.
- **Multi-Factor Authentication (MFA):** A security method requiring two or more verification factors to confirm a user's identity (e.g., password plus a code sent to a mobile device, biometric scan, or security token).
- **Data Wiping:** Data removal or erasure is the process of remotely removing or erasing data from a personal or corporate device when necessary to protect the organization's information. It is typically done if the device is lost, stolen, or poses a security threat.

RESPONSIBILITY

INFORMATION SECURITY GROUP (ISG) and IT Team

- Oversee the implementation of this policy.
- Ensure all employees understand their responsibilities when using personal devices for work.

Employees/Contractors

- Comply with the terms of this policy and any associated security guidelines.
- Maintain the security of personal devices used to access corporate data.

POLICY

BYOD-registered devices are subject to all of our information security-related policies and procedures. This policy is in addition to and should be read alongside our Acceptable Usage Policy.

Approval, registration, and support of devices

- **Supported Devices**
  - **Laptops:** Any model or manufacturer that provides the OS is still supported.
  - **Desktops:** Same as above.
  - **Mobile Devices (Smartphones):** Any model or manufacturer, provided the OS is supported.
  - **Tablets:** Any model or manufacturer that provides the OS is supported.
- **Registered Devices**
  - Only devices explicitly registered with the IT Department may access corporate data or systems.
  - Employees are responsible for notifying the IT Department of device changes or replacements.

Acceptable use of registered devices

Business and Personal Use

- **Acceptable business uses** include any activity that directly or indirectly supports organization objectives.
- **Limited personal use** is permitted during working hours, provided it does not interfere with duties or violate any policy.

Website and Application Restrictions

- Organizations may block or restrict access to specific categories of websites (e.g., adult content, gambling, peer-to-peer file sharing) during work hours or on the corporate network.
- Applications not downloaded through official stores (e.g., iTunes, Google Play, Microsoft Store) or from the developer's official website are prohibited.
- Storing or transmitting illicit materials or proprietary/confidential information.
- Harassing others or engaging in outside business activities that conflict with the organization's interests.
- **Permissible Work Assets Access** Employees may use registered devices to access the following:
  - Email
  - Calendars
  - Contacts
  - Documents and other authorized resources

Security

Password Protection

- Devices must be **password-protected** following the organization's Password Policy.
- An **automatic lock** must engage after five minutes of inactivity.

Device Restrictions

- Rooted (Android) or jailbroken (iOS) devices are strictly prohibited.
- Only registered devices can be used for organizational data access.

Logical Access Control

- The ACCESS CONTROL POLICY automatically limits employees' access to corporate information, ensuring least-privilege principles.

Device Maintenance

- Employees must keep operating systems, applications, and security patches current.
- If applicable, they must also comply with regulatory requirements for handling personal or sensitive data.

Device Loss or Theft

- Report lost or stolen devices to the ISG as soon as possible (within 24 hours).
- Immediately notify the mobile carrier to suspend service, if applicable.
- A device may be remotely wiped if:
    - It is lost or stolen.
    - It detects a policy breach or data compromise.
    - A virus or similar threat is discovered that endangers the organization's infrastructure.

Risks, Liabilities, and Disclaimers

- **Data Loss Precautions**
    - The organization may perform a remote wipe to protect corporate data. Personal data may be lost, so employees are responsible for backing up personal files.
- **Service Disconnection**
    - The organization may disconnect devices or turn off certain services when a security threat is suspected or during employee offboarding.
- **Personal Liability**
    - Employees bear all costs associated with their devices (e.g., carrier fees and data plans).
    - Employees must use registered devices ethically, adhering to the Acceptable Usage Policy.

Breaches of the Policy

The organization will take all necessary measures to address violations, including disciplinary action, legal remedies, or contractual enforcement where appropriate.

Annexure A - Guidelines

Physical Security

- Transport mobile devices in sturdy, waterproof, padded containers.
- Never leave devices unattended; secure them when away from desks.
- Keep devices out of sight (e.g., away from open windows) to reduce theft risk.
- The record makes models and serial numbers in the asset inventory.

Data Security

- Use approved operating systems with all relevant security patches.
- Keep OS/application patch levels consistent with organization standards.
- Regularly back up essential data; verify backups before wiping or reformatting storage.
- Unlicensed or pirated software is prohibited.
- Scan all external media (e.g., USB drives) with antivirus before use.
- Antivirus and Malware Tools
    - Install and update antivirus/anti-malware programs for real-time protection.
    - Run daily updates and at least one weekly scan.

When Traveling

- Keep mobile devices in sight; do not check them with baggage.
- During airport security checks, monitor devices to prevent theft or loss.
- Carry appropriate documentation when traveling internationally.

Network Security

- Before connecting to any network, verify that the antivirus is up-to-date and scan for malware.
- Remove any malware found before joining an organization's network; log and report the incident to the ISG.
- For devices not owned by the organization, the owner must agree in writing to allow scans or inspections as needed.

Version Details

Version	Version Date	Description of changes	Created By	Approved By	Published By
Version 1.0	Mar 14 2026	Initial Release	Pronoy	Kartikeya	Kartikeya