

PDS INFOTECH PVT LTD

Mobile Device Policy

Ref No: ISMS/PDS/5.2/1.2

1. Purpose

This policy outlines the use of mobile devices by employees of PDS Infotech Pvt Ltd ("the Company"), whether Company-owned or personally owned. It should be read and understood by all employees who use, or wish to use, a personal mobile device for work purposes; use a Company-owned mobile device; or bring a personal mobile device onto Company property.

2. Policy

2.1 Use of Personal Mobile Devices

- Employees may use personal devices for work purposes only when authorized in writing, in advance, by management, with the employee's written consent. Personal electronic devices include, but are not limited to, personally owned phones, tablets, laptops, and computers.
- Failure to follow this policy may result in disciplinary action, up to and including termination of employment.

2.2 Use of Company-Owned Mobile Devices

- Certain employees may be issued a Company-owned mobile device. Use of such devices is contingent upon continued employment with the Company, and the device remains the sole property of the Company.
- Company-provided mobile devices may be part of a corporate mobile plan with shared minutes and data usage. Excessive use of minutes or bandwidth for non-business activity is discouraged and may result in a payroll deduction for personal usage, applied in accordance with the Payment of Wages Act, 1936 and Company HR policy.

2.3 Security

- Employees must set a PIN, password, or other authentication measure on every device used to access Company information.
- Where possible, employees should use two-factor or two-step verification for added application/device security.
- Employees must not use cloud-based apps or backup services that transfer Company data to unapproved third parties; only IT-approved applications may be used for Company data.
- Devices used for work purposes must not be synchronized with other personal devices.
- Modifications to device hardware or software, or installation of additional hardware or software beyond routine updates, is prohibited unless approved by IT.
- Family members and friends must not use personal devices that are also used for Company purposes.
- Employees whose personal devices have camera, video, or recording capability must not use those functions on Company property unless authorized in advance by management.
- Employees must not store information relating to prior employment on a Company-owned device.

2.4 Behaviour

- Employees are expected to exercise the same discretion using personal devices for work purposes as is expected when using Company-owned devices. Company policies on harassment, discrimination, retaliation, trade secrets, confidentiality, and ethics apply equally to personal device use for work-related activity.

2.5 Privacy and Monitoring

- The Company may monitor and preserve communications that use Company networks or applications — including data, voicemail, telephone logs, and network traffic — regardless of the ownership status of the device, where reasonable, proportionate, and for a legitimate business or security purpose, consistent with the Digital Personal Data Protection Act, 2023.
- The Company may review, retain, or disclose personal and Company-related data on mobile devices in response to a lawful request from a regulatory or law enforcement authority, or in connection with legal proceedings.
- Employees must not knowingly disable any software or system identified as a Company monitoring or security tool.

2.6 Inspection

Employees may be asked to produce a mobile device used for work purposes for inspection, to confirm compliance with this policy.

2.7 Safety

- Employees whose duties involve driving must not use mobile devices while driving. Regardless of traffic conditions, employees must safely stop the vehicle before placing or accepting a call or message, unless the call is entirely hands-free.
- Employees charged with a traffic violation arising from mobile device use while driving are solely responsible for resulting liabilities.
- Employees working in hazardous areas must refrain from using mobile devices where doing so may present a safety hazard.

2.8 Lost, Stolen, Hacked, or Damaged Equipment

- Employees must protect mobile devices used for work purposes from loss, damage, or theft, and must notify management immediately if a device is lost or stolen.
- If a device is damaged, the employee must notify management immediately and will be responsible for the cost of repair or replacement.
- Employees may face disciplinary action, up to and including termination, for wilful damage to a Company-owned mobile device.

2.9 Termination of Employment

Upon resignation or termination of employment, the company device will be reset to factory defaults using the Company's remote wipe software. The Company is not responsible for loss or damage of personal applications or data resulting from this process.

3. Roles and Responsibilities

- IT Department: Installs and manages software, executes wipes, and approves hardware/software changes to devices. Authorizes personal device use for work purposes and approves exceptions to work-hour restrictions.
- All Personnel: Comply with this policy and report lost, stolen, or damaged devices immediately.

4. Review

This policy shall be reviewed at least annually, or upon significant organizational or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022 and applicable Indian law.