PDS INFOTECH PVT LTD

Asset Management Policy

Ref No: ISMS/PDS/5.2/19.1

1. Purpose

This policy establishes the rules for the control, classification, and lifecycle management of hardware, software, applications, and information used by PDS Infotech Pvt Ltd ("the Company"), in order to protect the confidentiality, integrity, and availability of the Company's information assets.

2. Scope / Audience

This policy applies to all individuals responsible for the use, purchase, implementation, or maintenance of the Company's information resources, including employees, contractors, and approved third parties acting on the Company's behalf.

3. Policy

3.1 Hardware, Software, Applications, and Data

- All hardware, software, and applications must be approved and purchased by Company IT.
- Installation of new hardware or software, or modification of existing hardware or software, must follow approved Company procedures and change control processes.
- All purchases must follow the Company's defined Technology Purchasing Standard.
- Software used by employees, contractors, and other approved third parties working on behalf of the Company must be properly licensed.
- Software installed on Company computing equipment, other than that listed in the Company's Standard Software List, must be approved by IT Management and installed by Company IT personnel.
- Only Company-authorized cloud computing applications may be used for sharing, storing, or transferring confidential or internal information.
- Use of cloud computing applications must comply with all applicable laws and regulations concerning the information involved, including personal data and sensitive personal data as defined under the Digital Personal Data Protection Act, 2023 and the SPDI Rules, 2011 (e.g. financial information, health records, biometric data, government-issued identifiers).
- Option for two-factor authentication for external cloud computing applications with access to any confidential information for which the Company has a custodial responsibility.
- Contracts with cloud computing application providers must address data retention, destruction, data ownership, and data custodian rights.
- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All Company assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner, managed by Company IT Management.
- Company assets exceeding a value threshold set by management must not be removed from Company premises without management approval.

- All Company physical assets exceeding a value threshold set by management must carry an asset tag or equivalent means of identifying the equipment as Company-owned.
- If a Company asset is being taken to a high-risk or sanctioned jurisdiction — as advised by Ministry of External Affairs (India) travel advisories or Company Security Guidelines — it must be inspected and approved by IT before being taken offsite and before reconnecting to the Company network.
- Confidential information must be transported only by a Company employee or an IT Management-approved courier.
- Upon termination of employment, contract, or agreement, all Company assets must be returned to Company IT Management.

3.2 Mobile Devices

- Use of a personally owned mobile device to connect to the Company network is a privilege granted to employees only upon formal approval by IT Management.
- Mobile devices that access Company email must have a PIN or other authentication mechanism enabled.

3.3 Media Destruction and Re-Use

- Media that may contain confidential or internal information must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must comply with the Company's Media Reuse and Destruction Standards.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, including encrypted media.

3.4 Backup

- The frequency and extent of backups must correspond to the importance of the information and the acceptable risk as determined by the information owner.
- The Company's backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
- Vendors providing offsite backup storage for the Company must be formally approved to handle the highest classification level of information stored.
- Physical access controls at offsite backup storage locations must meet or exceed those of the source systems. Backup media must be protected in accordance with the highest sensitivity level of information stored.
- A process must be implemented to verify the success of the Company's electronic information backups.
- Backups must be periodically tested to confirm they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between the Company and offsite backup storage vendor(s) must be reviewed at least annually.
- Backups containing confidential information must be encrypted in accordance with the Encryption Standard.
- Signature cards or equivalent access authorizations held by offsite backup storage vendor(s) for access to Company backup media must be reviewed annually, or when an authorized individual leaves the Company.
- Backup media must, at minimum, be identifiable by labels and/or a barcoding system carrying the following information:
    - System name.
    - Creation date.
    - Sensitivity classification.
    - Company contact information.

3.5 Removable Media

- Use of removable media to store Company information must be supported by a reasonable business case.
- All removable media use must be approved by Company IT prior to use.
- Personally owned removable media must not be used to store Company information.
- Users must not connect removable media of unknown origin without prior approval from Company IT.
- Confidential and internal Company information must not be stored on removable media without encryption.
- Loss or theft of removable media that may have contained Company information must be reported to Company IT immediately.
- The Company will maintain inventory logs of all media and conduct media inventories annually.

4. Related Documents

- Information Classification and Management Policy
- Media Reuse and Destruction Standard
- Technology Purchasing Standard

5. Roles and Responsibilities

- IT Management: Approves and procures hardware/software/applications, maintains asset inventories, manages backups and media destruction, and enforces this policy.
- Information Owners: Determine backup frequency, classification, and retention requirements for information under their ownership.
- All Personnel: Comply with this policy and promptly report lost, stolen, or damaged assets and media to IT.

6. Review

This policy shall be reviewed at least annually, or upon significant organizational, technological, or regulatory change, to ensure continued alignment with ISO/IEC 27001:2022 and applicable Indian law, including the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the SPDI Rules, 2011.