

PDS INFOTECH PVT LTD

Asset Management Policy (Ref No: - ISMS/PDS/5.2/19)

Purpose

The purpose of the (PDS INFOTECH PVT LTD) Asset Management Policy (Ref No: - ISMS/PDS/5.2/19) is to establish the rules for the control of hardware, software, applications, and information used by (PDS INFOTECH PVT LTD).

Audience

The (PDS INFOTECH PVT LTD) Asset Management Policy (Ref No: - ISMS/PDS/5.2/19) applies to individuals who are responsible for the use, purchase, implementation, and/or maintenance of (PDS INFOTECH PVT LTD) Information Resources

Policy

Hardware, Software, Applications, and Data

- All hardware, software and applications must be approved and purchased by (PDS INFOTECH PVT LTD) IT.
- Installation of new hardware or software, or modifications made to existing hardware or software must follow approved (PDS INFOTECH PVT LTD) procedures and change control processes.
- All purchases must follow the defined (PDS INFOTECH PVT LTD) (Technology) Purchasing Standard.
- Software used by (PDS INFOTECH PVT LTD) employees, contractors and/or other approved third parties working on behalf of (PDS INFOTECH PVT LTD), must be properly licensed.
- Software installed on (PDS INFOTECH PVT LTD) computing equipment, outside of that noted in the (PDS INFOTECH PVT LTD) Standard Software List, must be approved by IT Management and installed by (PDS INFOTECH PVT LTD) IT personnel.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g. personally identifiable information (PII), protected health information (PHI), corporate financial data, etc.
- Two-factor authentication is required for external cloud computing applications with access to any confidential information for which (PDS INFOTECH PVT LTD) has a custodial responsibility.
- Contracts with cloud computing applications 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 (PDS INFOTECH PVT LTD) assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by (PDS INFOTECH PVT LTD) IT Management.

- (PDS INFOTECH PVT LTD) assets exceeding a set value, as determined by management, are not permitted to be removed from (PDS INFOTECH PVT LTD)'s physical premises without management approval.
- All (PDS INFOTECH PVT LTD) physical assets exceeding a set value, as determined by management, must contain asset tags or a similar means of identifying the equipment as being owned by (PDS INFOTECH PVT LTD).
- If a (PDS INFOTECH PVT LTD) asset is being taken to a High-Risk location, as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the (PDS INFOTECH PVT LTD) network.
- Confidential information must be transported either by an (PDS INFOTECH PVT LTD) employee or a courier approved by IT Management.
- Upon termination of employment, contract, or agreement, all (PDS INFOTECH PVT LTD) assets must be returned to (PDS INFOTECH PVT LTD) IT Management.

Mobile Devices

- (PDS INFOTECH PVT LTD) does not allow personally owned mobile devices to connect to the (PDS INFOTECH PVT LTD) corporate internal network.

OR

- The use of a personally owned mobile devices to connect to the (PDS INFOTECH PVT LTD) network is a privilege granted to employees only upon formal approval of IT Management.
- Mobile devices used to connect to the (PDS INFOTECH PVT LTD) network are required to use the approved Mobile Device Management (MDM) solution.
- Mobile devices that access (PDS INFOTECH PVT LTD) email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the (PDS INFOTECH PVT LTD) Encryption Standard.
- All mobile devices should maintain up-to-date versions of all software and applications.

Media Destruction & 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 be conducted in compliance with (PDS INFOTECH PVT LTD)'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, included encrypted media.

Backup

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The (PDS INFOTECH PVT LTD) backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule.
- The vendor(s) providing offsite backup storage for (PDS INFOTECH PVT LTD) must be formally approved to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest (PDS INFOTECH PVT LTD) sensitivity level of information stored.

- A process must be implemented to verify the success of the (PDS INFOTECH PVT LTD) electronic information backup.
- Backups must be periodically tested to ensure that 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 (PDS INFOTECH PVT LTD) and the 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 held by the offsite backup storage vendor(s) for access to (PDS INFOTECH PVT LTD) backup media must be reviewed annually or when an authorized individual leaves (PDS INFOTECH PVT LTD).
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
 - System name
 - Creation Date
 - Sensitivity Classification
 - (PDS INFOTECH PVT LTD) Contact Information

Removable Media

- The use of removable media for storage of (PDS INFOTECH PVT LTD) Information must be supported by a reasonable business case.
- All removable media use must be approved by (PDS INFOTECH PVT LTD) IT prior to use.
- Personally owned removable media use is not permitted for storage of (PDS INFOTECH PVT LTD) information.
- Users are not permitted to connect removable media from an unknown origin, without prior approval from (PDS INFOTECH PVT LTD) IT.
- Confidential and internal (PDS INFOTECH PVT LTD) information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained any (PDS INFOTECH PVT LTD) information must be reported to the (PDS INFOTECH PVT LTD) IT.
- (PDS INFOTECH PVT LTD) will maintain inventory logs of all media and conduct media inventories at least annually.
- The transfer of information to removable media will be monitored.
- Encryption Standard
- Information Classification and Management Policy
- Media Reuse and Destruction Standard
- Technology Purchasing Standard