PDS INFOTECH PVT LTD

Removable Media Policy

Ref No: ISMS/PDS/5.2/15.1

1. Policy Statement

PDS Infotech Pvt Ltd ("the Company") will ensure the controlled use of removable media devices to store and transfer information by all users who have access to information, information systems, and IT equipment for the purpose of conducting official Company business.

2. Purpose

This policy establishes the principles and working practices to be adopted by all users so that data is safely stored and transferred on removable media. It aims to ensure that use of removable media devices is controlled in order to:

- Maintain the integrity of the data. Enable correct data to be made available where required.
- Prevent unintended or deliberate harm to the stability of the Company's computer network.
- Build confidence and trust in data shared between systems.
- Maintain high standards of care in securing Proprietary, Client Confidential, and Company Confidential information, as defined in the Information Classification Policy.

3. Scope

This policy applies to all employees, departments, contractual third parties, and agents of the Company who have access to Company information, information systems, or IT equipment, and who intend to store information on removable media devices.

4. Definition

Removable media devices include, but are not restricted to, the following:

- External hard drives.
- USB memory sticks (pen drives / flash drives).
- Media card readers.
- CDs, DVDs, and optical disks.
- Embedded microchips, including smart cards and mobile phone SIM cards.
- Digital cameras.
- Backup cassettes and audio tapes (including Dictaphones and answering machines).

5. Risks

The Company recognizes that risks are associated with users accessing and handling information to conduct official Company business. Securing Proprietary, Client Confidential, and Company Confidential data is of paramount importance, particularly given the Company's obligations under the Digital Personal Data Protection Act, 2023. Loss of access to information, or interference with its integrity, could significantly affect the Company's operations. This policy aims to mitigate the following risks:

- Disclosure of confidential information as a consequence of loss, theft, or careless use of removable media.

- Contamination of Company networks or equipment through viruses introduced during data transfer between devices.
- Potential sanctions against the Company or individuals imposed by the Data Protection Board of India as a result of information loss or misuse.
- Potential legal action against the Company or individuals as a result of information loss or misuse.
- Reputational damage to the Company as a result of information loss or misuse.

Non-compliance with this policy could significantly affect the Company's operations and may result in financial loss and an inability to serve customers effectively.

6. Applying the Policy

6.1 Restricted Access to Removable Media

- The Company’s policy is to prohibit use of removable media by default. Use will only be approved where a valid business case is developed and demonstrates that the benefits clearly outweigh the associated risks.
- Requests for access to, and use of, removable media devices must be made to IT Management. Approval must be given by IT Management or the Information Security Committee.

6.2 Procurement of Removable Media

- All removable media devices, and any associated equipment or software, must be purchased and installed only by IT.
- Non-Company-owned removable media devices must not be used to store information related to Company business, and must not be connected to any Company-owned or leased IT equipment.
- Only equipment and media purchased by the Company and approved by IT Management may be connected to Company equipment or the Company network.

6.3 Security of Data

- Removable media must not be the sole location where Company data is held. Copies of data stored on removable media must remain on the source system or networked computer until successfully transferred to another networked computer or system.
- To minimize physical risk, loss, theft, or corruption, all storage media must be stored in an appropriately secure environment.
- Each user is responsible for the appropriate use and security of data, and for not allowing removable media devices or the information on them to be compromised while in their care or control.
- All data stored on removable media devices must, where possible, be encrypted. Where full encryption is not possible, all Client Confidential and Company Confidential data held on the device must be encrypted, in accordance with the Cryptographic Control and Management Policy.
- Users should be aware that the Company will audit and log the transfer of data files to and from removable media devices and Company-owned IT equipment.

6.4 Incident Management

All users should immediately report any actual or suspected information security breach involving removable media to IT Management, in accordance with the Data Breach Policy.

6.5 Third-Party Access to Company Information

- No third party (external contractors, partners, agents, or other non-employees) may receive data or extract information from the Company's network, information stores, or IT equipment without explicit agreement from IT.

- Where third parties are permitted access to Company information, all provisions of this policy apply to their storage and transfer of that data.

6.6 Preventing Information Security Incidents

- Damaged or faulty removable media devices must not be used. Users must contact IT Management if removable media becomes damaged.
- Approved virus and malware checking software must be operational on both the source machine and the receiving machine. Data must be scanned by two functionally different virus-checking products before the media is loaded onto the receiving machine.
- Data held on removable media in transit or storage must be given security appropriate to its sensitivity. Encryption or password protection must be applied unless there is no risk to the Company or affected individuals from the data being lost in transit or storage.

6.7 Disposing of Removable Media Devices

- Removable media devices that are no longer required, or have become damaged, must be disposed of securely to prevent data leakage.
- Removable media devices that are no longer required, or have become damaged, must be returned to IT for secure disposal.

6.8 User Responsibility

All provisions of this policy must be adhered to at all times. Special attention must be paid to the following:

- Only Company-supplied and IT-approved removable media may be used in connection with Company equipment, the Company network, or Company business information.
- Data stored on removable media must be encrypted where possible.
- Virus and malware checking software must be used whenever removable media is connected to a machine.
- Only data that is authorized and necessary should be saved to removable media.
- Special care must be taken to physically protect the device and its data from loss, theft, or damage during transport.

7. Policy Compliance

Any user found to have breached this policy may be subject to disciplinary procedure. Where a criminal offence is considered to have occurred, further action may be taken to support prosecution of the offender(s). Anyone unsure how this policy applies to them should seek advice from IT.

8. 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.