PDS INFOTECH PVT LTD

Cryptographic Control and Management Policy

Ref No: ISMS/PDS/5.2/4.1

1. Purpose

This policy defines the requirements for the use of cryptographic controls to protect the confidentiality, integrity, and authenticity of information owned or processed by PDS Infotech Pvt Ltd ("the Company"), whether that information resides on Company-managed infrastructure, employee devices, or third-party/cloud service provider platforms.

2. Scope

This policy applies to all information systems, applications, devices, and storage media owned, operated, or used by the Company, including infrastructure and services provided by third-party vendors such as AWS, Microsoft, Google, Zoho, Freshdesk, GoDaddy, and similar service providers. It applies to all employees, contractors, and third parties who handle Company information.

3. Policy

3.1 Use of Encryption

- Confidential and sensitive information, including personal data as defined under the Digital Personal Data Protection Act, 2023, should be encrypted both in transit and at rest, wherever technically feasible.
- Data in transit over public networks, including the Internet, should be protected using an industry-standard secure protocol.
- Data at rest on servers, databases, laptops, and removable media containing confidential or sensitive information should be encrypted using an approved encryption method.
- Email containing confidential or sensitive information must be sent using an approved secure or encrypted messaging solution, in line with the Acceptable Use Policy.

3.2 Approved Algorithms and Standards

- Only industry-recognized, non-deprecated cryptographic algorithms and key lengths may be used. Deprecated or weak algorithms and protocols must be phased out of use where identified.
- IT Management is responsible for maintaining a current list of approved algorithms, protocols, and minimum key lengths, reviewed periodically to reflect evolving industry standards.

3.3 Key Management

- Cryptographic keys must be generated, stored, distributed, rotated, and revoked in a secure manner, with access restricted to authorized personnel only.
- Keys should not be stored alongside the data they protect, except where a cloud provider's managed key service is used under a documented shared-responsibility model.
- Where a cloud provider's native key management service is used, responsibility for key management must be clearly documented, and access to key management consoles must be restricted and logged.
- Cryptographic keys should be rotated periodically and promptly upon suspected compromise or when an authorized key holder leaves the Company.

- Loss, compromise, or suspected compromise of a cryptographic key must be reported immediately to IT Management and handled in accordance with the Incident Management Policy.

3.4 Third-Party and Cloud Service Provider Encryption

- Where core business applications and infrastructure are hosted with third-party service providers, the Company relies in part on the encryption capabilities offered by these providers.
- Before onboarding a new third-party or cloud service provider for handling confidential or sensitive information, IT Management should verify that the provider offers adequate encryption at rest and in transit, and that contractual terms address data protection responsibilities.
- Reliance on a third-party provider's encryption does not remove the Company's own obligation to apply appropriate cryptographic controls to information under its direct control, such as endpoint devices, internally developed applications, exported data, and removable media.
- IT Management should periodically review third-party providers' security and encryption practices to confirm continued alignment with this policy.

3.5 Compliance

- Use of cryptographic controls must comply with applicable Indian law, including the Information Technology Act, 2000 and its rules, and any sector- or licence-specific restrictions on encryption strength that may apply to the Company's operations.
- Where cryptographic controls are used to protect personal data, such use must support the Company's obligations under the Digital Personal Data Protection Act, 2023.

4. Roles and Responsibilities

- IT Management: Maintains the approved algorithm/protocol list, manages encryption implementation and key management, and evaluates third-party provider encryption practices.
- Information Security Committee: Owns this policy and approves exceptions.
- All Personnel: Use only approved encryption methods and tools, and report any suspected key compromise or cryptographic failure immediately.

5. Review

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