PDS INFOTECH PVT LTD

Information Security Policy for Supplier Relationships

Ref No: ISMS/PDS/5.2/9.1

1. Purpose

This policy defines how PDS Infotech Pvt Ltd ("the Company") manages information security risk arising from its relationships with suppliers, vendors, and service providers, including cloud and SaaS providers, to ensure that information accessed, processed, or stored by third parties is adequately protected.

2. Scope

This policy applies to all suppliers, vendors, contractors, and service providers — including cloud/SaaS platforms, IT service providers, professional services firms, and any other third party — that access, process, store, or transmit Company information, or that connect to Company systems.

3. Policy

3.1 Supplier Categorization and Risk Assessment

- Before onboarding any new supplier with access to Company information or systems, IT Management or the engaging function must assess the supplier's information security risk based on the type of data involved, the level of system access required, and the supplier's own security policies.
- Established global cloud and SaaS providers (including AWS, Microsoft, Google, Zoho, Freshdesk, GoDaddy) are assessed against their published security certifications and compliance documentation as part of this process.
- All other suppliers, regardless of size, must undergo a risk assessment before being granted any access to Company information or systems; no supplier is exempt from this policy by default.

3.2 Security Requirements in Supplier Agreements

- Contracts or agreements with suppliers who access Company information must include applicable security requirements, proportionate to the assessed risk level, covering matters such as confidentiality, data protection, breach notification, and the right to audit where appropriate.
- Where a supplier processes personal data on the Company's behalf, the agreement must address the parties' respective obligations under the Digital Personal Data Protection Act, 2023.
- Supplier access to Company systems must be limited to what is strictly necessary for the contracted service, following the principle of least privilege set out in the Access Control Policy.

3.3 Ongoing Monitoring and Review

- Significant changes to a supplier's services, ownership, or security practices must trigger a re-assessment of the associated risk.
- Any security incident involving a supplier must be handled in accordance with the Data Breach Policy.

3.4 Offboarding

- When a supplier relationship ends, all supplier access to Company systems and information must be revoked promptly.

- The Company must confirm the return or secure destruction of Company information held by the supplier, in accordance with the Media Reuse and Destruction Standard where applicable.

4. Roles and Responsibilities

- IT: Conducts supplier risk assessments, manages technical access for suppliers, and coordinates offboarding.
- All Personnel: Only grant supplier access to Company information based on the regulations stated in this policy.

5. 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.