PDS INFOTECH PVT LTD

Access Control Policy

Ref No: ISMS/PDS/5.2/2.1

1. Purpose

This policy defines the principles and controls governing access to PDS Infotech's confidential and sensitive information, whether held in physical or digital form, to ensure that access is granted only to authorized personnel on a need-to-know and least-privilege basis.

2. Scope

This policy applies to all employees, contractors, and third parties who access PDS Infotech's information assets, whether stored physically or digitally, across all business locations.

3. Policy Statement

Access to confidential and sensitive information is restricted to authorized personnel only. Access rights are granted based on job role and business need, and are reviewed periodically to ensure continued appropriateness.

3.1 Physical Access

Physical records containing confidential or sensitive information are stored under lock and key within designated office premises or approved offsite storage locations. Access to these materials is restricted to personnel explicitly authorized by the Information Security Committee / Top Management, and is logged where applicable.

3.2 Digital Access

- Download or export functionality for sensitive information is disabled by default for operational-level users across applications and systems.
- Elevated or full access privileges are granted only to designated personnel, based on documented approval from the Information Security Committee / Top Management.
- Access rights are assigned following the principle of least privilege and are reviewed on a periodic basis (at least annually, or upon role change).

4. Roles and Responsibilities

- Top Management / Information Security Committee: Approves access levels for sensitive and confidential information.
- IT/Systems Team: Implements and maintains technical access controls (e.g., download restrictions, user permissions).
- Employees: Responsible for safeguarding any access granted and reporting suspected unauthorized access.

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 requirements.