PDS INFOTECH PVT LTD

Information Access Restriction Policy

Ref No: ISMS/PDS/5.2/3.1

1. Purpose

This policy defines how access to PDS Infotech Pvt Ltd.'s ("the Company") information — in both physical and digital form — is restricted according to the classification level of that information. It complements the Access Control Policy (Ref No: ISMS/PDS/5.2/2), which defines the roles, approval process, and review cadence for granting access; this policy defines what level of restriction applies to information based on its classification.

2. Scope

This policy applies to all physical and digital information assets held by the Company, and to all employees, contractors, and third parties who access them.

3. Policy

Access to information, whether in physical or digital format, is made available to personnel in a restrictive manner, based on the classification of the information and the scope of the individual's area of responsibility, in accordance with the Information Classification and Management Policy.

3.1 Physical Information

- Documents classified for general business use are freely accessible to personnel who require them for day-to-day business operations.
- Documents classified as confidential are subject to restricted access and must be protected under lock and key.
- Authorization to access confidential physical information is vested in designated personnel, as approved by top management / the Information Security Committee, in accordance with the Access Control Policy.

3.2 Digital Information

- Digital information classified for general business use is freely accessible to personnel who require it for day-to-day business operations.
- Digital information classified as confidential is subject to restricted access and must be protected using unique user IDs and passwords, and multi-factor authentication where available.
- Authorization to access confidential digital information is vested in designated personnel, as approved by top management / the Information Security Committee, in accordance with the Access Control Policy.
- Access rights to confidential digital information must be reviewed periodically to ensure continued appropriateness, in line with the Access Control Policy.

4. Roles and Responsibilities

- Information Security: Approves individual access to confidential physical and digital information.
- IT Management: Implements and maintains technical access restrictions for digital information (user IDs, passwords, permissions).
- All Personnel: Respect information classification and access restrictions, and report any 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.