PDS INFOTECH PVT LTD

Information Classification and Management Policy

Ref No: ISMS/PDS/5.2/13.1

1. Purpose

PDS Infotech Pvt Ltd ("the Company") provides fast, efficient, and cost-effective software services to clients worldwide. It is critical for the Company to set a clear standard for the protection of information assets from unauthorized access, compromise, or disclosure. This policy establishes the Company's information classification system to help manage and protect its information assets.

2. Scope

This policy applies to all information owned by the Company and all information entrusted to the Company by third parties, in physical or digital form, and to all employees, contractors, and third parties who handle it.

3. Policy

- All Company associates share responsibility for ensuring that Company information assets receive an appropriate level of protection by observing this policy.
- Managers or information "owners" are responsible for assigning classifications to information assets according to the classification system below.
- Where practicable, the classification category shall be embedded in the information itself (e.g. document headers/footers, file naming, or metadata).
- All associates shall be guided by the assigned classification in their security-related handling of Company information.

All Company information, and all information entrusted to the Company by third parties, falls into one of four classifications, presented below in order of increasing sensitivity.

3.1 Classification Levels

Information Category	Description	Examples
Unclassified Public	Information is not confidential and can be made public without implications for the Company. Loss of availability due to system downtime is an acceptable risk.	▪ Widely distributed product brochures. ▪ Information already available in the public domain, including public Company website areas. ▪ Sample downloads of Company software offered for sale. ▪ Statutory financial statements filed with the regulatory authorities. ▪ Newsletters intended for external transmission.
Proprietary	Information restricted to management-approved internal access and protected from external access. Unauthorized access could affect operational effectiveness, cause financial loss, provide a significant	▪ Passwords and corporate security procedure information. ▪ Know-how used to process client information.

	gain to a competitor, or damage customer confidence.	▪ Standard Operating Procedures used across the Company's business. ▪ Company-developed software code, whether used internally or sold to clients.
Client Confidential Data	Information received from clients, for processing in production by the Company. The original copy of such information must not be changed in any way without the client's written permission.	▪ Client-provided media, electronic transmissions from clients. ▪ Product information generated for the client by the Company based on production activities specified by the client.
Company Confidential Data	Information collected and used by the Company to employ people, log and fulfil client orders, and manage corporate finance. Access is restricted within the Company.	▪ Salaries and other personnel data. ▪ Accounting data and internal financial reports. ▪ Confidential customer business data and confidential contracts. ▪ Non-disclosure agreements with clients/vendors. ▪ Company business plans.

4. Roles and Responsibilities

- Information Owners: Review the classification of information under their ownership periodically.
- Information Security team: Conduct initial data classification, and review periodically. Approve reclassification requests/decisions.

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.