PDS INFOTECH PVT LTD

Employee Confidentiality Policy

Ref No: ISMS/PDS/5.2/12.1

1. Purpose

This policy explains how PDS Infotech Pvt Ltd ("the Company") expects employees to treat confidential information. Employees will unavoidably receive and handle personal and private information about clients, partners, and the Company, and the Company requires that this information be well protected.

This information must be protected for two reasons. It may:

- Be legally binding (e.g. sensitive customer data, personal data under the Digital Personal Data Protection Act, 2023).
- Constitute the backbone of the Company's business, giving it a competitive advantage (e.g. business processes, pricing strategy).

2. Scope

This policy applies to all employees, including board members, investors, contractors, and volunteers, who may have access to confidential information.

3. Policy Elements

Confidential and proprietary information is secret, valuable, and sensitive. Common examples of confidential information include:

- Unpublished financial information.
- Data of customers, partners, or vendors.
- Patents, formulas, or new technologies.
- Customer lists (existing and prospective).
- Data entrusted to the Company by external parties.
- Pricing, marketing, and other undisclosed strategies.
- Documents and processes explicitly marked as confidential.
- Unpublished goals, forecasts, and initiatives marked as confidential.

Employees may have varying levels of authorized access to confidential information, based on role and business need.

3.1 What Employees Should Do

- Lock or secure confidential information at all times.
- Shred confidential documents when they are no longer needed, in accordance with the Media Reuse and Destruction Standard.
- View confidential information only on secure, Company-approved devices.
- Disclose information to other employees only when necessary and authorized.
- Keep confidential documents within Company premises.

3.2 What Employees Should Not Do

- Use confidential information for personal benefit or profit.

- Disclose confidential information to anyone outside the Company without authorization.
- Replicate confidential documents and files or store them on insecure devices.

When employees stop working for the Company, they are obliged to return any confidential files and delete them from personal devices, in accordance with the Clear Desk, Clear Screen & Device Commissioning Policy.

3.3 Confidentiality Measures

The Company will take measures to ensure confidential information is well protected, including to:

- Store and lock paper documents.
- Encrypt electronic information and safeguard databases, in accordance with the Cryptographic Control and Management Policy.
- Require employees to sign confidentiality/non-disclosure agreements (NDAs) as a condition of access to confidential information.
- Require authorization from senior management before granting access to certain categories of confidential information.

3.4 Exceptions

Confidential information may occasionally need to be disclosed for legitimate reasons, for example:

- If a regulatory body (e.g. Data Protection Board of India) requests it as part of an investigation or audit.
- If the Company examines a venture or partnership that requires disclosing some information, within legal boundaries.

In such cases, the employees involved should document the disclosure procedure followed and collect all necessary authorizations. Disclosure must be limited to what is strictly necessary.

4. Disciplinary Consequences

Employees who do not respect this policy will face disciplinary action, and possibly legal action, in accordance with the Company's disciplinary procedures and applicable Indian labour law. The Company will investigate every reported breach of this policy. Employees who wilfully or repeatedly breach these confidentiality requirements, including for personal profit, are subject to disciplinary action up to and including termination, following due process and a fair inquiry. Unintentional breaches will be assessed based on their frequency and seriousness, and addressed proportionately in accordance with the Company's disciplinary procedures.

5. Roles and Responsibilities

- Senior Management: Authorizes access to confidential information, approves disclosure exceptions, manages NDA execution.
- Information Security: Owns this policy and advises on classification of confidential information.
- All Personnel: Comply with this policy and report suspected breaches promptly.

6. 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 and applicable Indian law.