PDS INFOTECH PVT LTD

Information Backup Policy

Ref No: ISMS/PDS/5.2/7.1

1. Purpose

This policy defines PDS Infotech Pvt Ltd's ("the Company") approach to backing up information across its digital environment, to ensure that data can be recovered in the event of loss, corruption, or system failure. It sets out the Company's backup strategy at the endpoint, office server, and cloud/vendor level. Detailed operational backup controls (frequency, testing, retention, encryption, offsite vendor requirements) are defined in the Asset Management Policy; this policy defines the overall strategy and the boundaries of the Company's reliance on third-party providers.

2. Scope

This policy applies to all information systems, applications, and devices used to store or process Company information, including individual endpoint devices, office servers, and third-party cloud service providers.

3. Policy

3.1 Third-Party Service Providers

- Most of the Company's core business digital applications and online infrastructure services are provided by established third-party service providers, including Amazon (AWS), Microsoft, Google, Zoho, Freshdesk, and GoDaddy.
- These providers maintain their own data/information backup, allowing data to be restored in the event of an exigency, and provide data export functionality that can serve as an additional backup mechanism or support data migration to another platform.
- The Company needs to parallelly ensure that critical business data is recoverable, and needs to maintain independent backups.

3.2 Internal Backup Tiers

The Company maintains a defined information backup approach across three tiers:

- Individual system (endpoint): Backup of data held on employee laptops/workstations.
- Office server level: Backup of data held on Company-managed on-premises or office infrastructure.
- External cloud storage level: Backup of data held with third-party cloud service providers.

For each tier, IT is responsible for defining and documenting the backup frequency, retention period, and recovery point/recovery time objectives (RPO/RTO) applicable to the systems, in accordance with the backup section of the Asset Management Policy.

3.3 Recovery and Testing

- Backups across all tiers must be periodically tested to confirm that data can be successfully restored, in accordance with the Asset Management Policy.
- Any failure identified during backup testing must be reported to IT Management and remediated promptly.
- Recovery procedures must be documented and accessible to authorized personnel in the event of a system failure or data loss incident.

4. Roles and Responsibilities

- IT: Defines and documents backup frequency, retention, and RPO/RTO for each tier; verifies third-party provider backup adequacy; conducts recovery testing.
- All Personnel: Store Company data only in approved locations (managed endpoints, office servers, or approved cloud applications) to ensure it falls within the defined backup scope.

5. Review

This policy shall be reviewed at least annually, or upon significant organizational or technological change, to ensure continued alignment with ISO/IEC 27001:2022.