



DIMENSION FINANCIAL SOLUTIONS PRIVATE LIMITED

12.5 – Data backup, storage and security

1. Data Storage Overview

- **Cloud Storage:**
All company data is stored in **OneDrive**, which synchronizes data in real time to ensure high availability and redundancy.
- **Physical NAS (Network Attached Storage):**
Critical and non-critical data are consolidated and securely stored on **NAS Server**, which serves as a central repository for all departments.

2. Access and Permissions

- **Departmental Access:**
 - Each department has exclusive access to its own data.
 - Cross-departmental access is restricted to prevent unauthorized viewing, editing, or deletion of data.
 - On recommendation of the department head, IT manager may allow access of certain data or files to employees based on their requirements.
- **Administrative Access:**
 - The administrator (**IT Manager**) holds full control over all data.
 - Responsibilities include:
 - Reading and writing data across all departments.
 - Managing user roles and permissions.
 - Enforcing data access controls.
- **Cloud:**
 - Employees only have access to their data.

3. Data Retention Policy

- **Standard Retention:**
All data is retained for **8 years** in compliance with regulatory and operational requirements.
- **Permanent Retention:**
Data classified as **critical** to the company is retained permanently on the NAS Server to ensure long-term availability.

4. Security and Synchronization

- **OneDrive:**
Real-time synchronization ensures data is always up to date and recoverable in case of hardware failure.
- **NAS Server:**
 - Designed for high reliability and scalability.
 - Regular backups protect against data loss.
- **User Permissions:**
Role-based access ensures that employees only interact with data necessary for their job functions, minimizing security risks.

For Dimension Financial Solutions Pvt. Ltd.

Director

