# Data Privacy & Encryption Strategy

## ✅ Anonymization Techniques

* • Tokenization of Sensitive Identifiers

Replace sensitive data (e.g., PAN, SSN) with non-sensitive equivalents (tokens). Tokens maintain data format but have no exploitable value outside the system.

* • Pseudonymization of Personal Data

Replace identifying fields with artificial identifiers or pseudonyms. Allows partial reversibility with a secure mapping table.

* • Differential Privacy for Analytical Purposes

Introduce mathematical noise into datasets to protect individual records. Enables aggregate data analysis without revealing personal details.

* • Dynamic Data Masking

Hide sensitive information in real-time based on user role or access level. Useful in UAT/test environments or dashboards.

## 🔐 Encryption Strategies

### 1. Data at Rest

* • AES-256 Encryption

Industry-standard symmetric encryption for databases, files, and backups.

* • Column-level Encryption

Encrypt specific sensitive fields like passwords, credit card numbers, etc.

* • Full Disk Encryption

Protects the entire storage volume (OS, logs, swap space) from physical access breaches.

### 2. Data in Transit

* • TLS 1.3 Encryption

Secures HTTP traffic (HTTPS), API communication, and client-server interactions.

* • Secure VPN for Remote Access

Encrypts remote connections from users and employees to internal systems.

### 3. End-to-End Encryption (E2EE) for Digital Banking

* • End-to-End Encryption

Ensures data remains encrypted throughout the transmission journey—from sender to receiver. Only endpoints can decrypt, preventing access from intermediaries (even servers).