**Data Privacy and Encryption Implementation**

**Name:** Nandhitha.S  
**Roll No.:** 713322AD070

**Data Privacy and Encryption**

To ensure the highest standards of data protection, the following data privacy techniques and encryption strategies will be implemented:

**Anonymization Techniques**

1. **Tokenization of Sensitive Identifiers**  
   Replaces sensitive data such as account numbers and SSNs with non-sensitive placeholders (tokens), ensuring that original values are stored securely in a token vault.
2. **Pseudonymization of Personal Data**  
   Transforms personal identifiers like names and emails into pseudonyms to prevent direct identification, while still allowing for data analytics.
3. **Differential Privacy for Analytical Purposes**  
   Adds random noise to datasets to preserve user privacy during data analysis, ensuring individual data points cannot be re-identified.
4. **Dynamic Data Masking**  
   Automatically hides sensitive data fields at query time for unauthorized users, displaying only masked values.

**Encryption Strategies**

**Data at Rest:**

* **AES-256 Encryption**: Industry-standard symmetric key encryption for files and databases.
* **Column-Level Encryption**: Encrypts specific sensitive fields such as passwords, financial details, and PII.
* **Full Disk Encryption**: Encrypts the entire disk storage, protecting data even if hardware is stolen.

**Data in Transit:**

* **TLS 1.3 Encryption**: Secures communications between clients and servers with the latest TLS protocol.
* **Secure VPN for Remote Access**: Provides encrypted tunnels for employees accessing data offsite.
* **End-to-End Encryption for Digital Banking**: Ensures data is encrypted from the user's device to the banking server, preventing interception at any point.

These privacy-preserving technologies will ensure that all sensitive information remains confidential and secure throughout its lifecycle.