Data Governance Framework

1. Governance Structure

- Chief Data Officer (CDO)

Leads the development and implementation of enterprise-wide data governance strategies. Owns data policies and oversees compliance with internal and external data standards.

- Chief Information Security Officer (CISO)

Ensures information security policies are enforced. Implements security controls and oversees incident response planning.

- Compliance Manager

Ensures compliance with regulations (GDPR, HIPAA). Coordinates audits and advises on legal risks.

- Data Stewards

Maintain data quality and resolve issues within domains like Finance, HR, etc.

2. Data Classification Policy

- Public Data

Non-sensitive information (e.g., marketing brochures). Minimal controls required.

- Internal Data

Information for internal use only (e.g., HR policies). Requires access control.

- Confidential Data

Customer financial information. Requires encryption and limited access.

- Highly Sensitive Data

Personal IDs, transaction details. Requires strong encryption, MFA, and monitoring.

3. Data Lifecycle Management

- Creation

Validated input mechanisms ensure high data quality.

- Storage

Encrypted and segregated storage to protect data.

- Access

Role-Based Access Control (RBAC) with MFA and audit logs.

- Retention

- Transaction Records: 7 years
- Customer Records: 10 years post-account closure
- Loan Documents: Life of loan + 7 years

4. Review and Compliance

This policy is reviewed annually or upon major changes. All employees must comply. Non-compliance may lead to access revocation or disciplinary action.