# Data Governance Framework

## 1. Purpose

This document establishes a Data Governance Framework to ensure data integrity, security, compliance, and lifecycle management within the organization.

## 2. Governance Structure

The governance structure assigns clear roles and responsibilities:

|  |  |
| --- | --- |
| Role | Responsibility |
| Chief Data Officer (CDO) | Oversees data strategy and governance. |
| Chief Information Security Officer (CISO) | Manages data security and access controls. |
| Compliance Manager | Ensures regulatory compliance (GDPR, HIPAA, PCI DSS). |
| Data Stewards | Manage data quality and integrity for respective domains. |

## 3. Data Classification

Data is categorized based on sensitivity and access requirements:

|  |  |  |
| --- | --- | --- |
| Category | Description | Access Control |
| Public Data | Non-sensitive, publicly available data | Open access |
| Internal Data | Restricted organizational information | Employees only |
| Confidential Data | Sensitive customer and business data | Limited to authorized teams |
| Highly Sensitive Data | Personally identifiable and financial data | Encrypted & strict access control |

## 4. Data Lifecycle Management

Data follows a structured lifecycle for security and compliance:

• Creation: Enforced input validation and metadata tagging.

• Storage: Data encryption and segregated storage for sensitive information.

• Access Control: Role-Based Access Control (RBAC) with strict permissions.

• Retention Policies:

- Transaction records – 7 years

- Customer records – 10 years post-account closure

- Loan documents – Life of loan + 7 years

• Secure Deletion: Expired data is permanently deleted using secure methods.

## 5. Compliance & Audits

The framework ensures adherence to data regulations such as:

✅ GDPR – EU data privacy regulations

✅ HIPAA – Healthcare data protection

✅ PCI DSS – Payment card security standards

Regular audits and monitoring are conducted to ensure compliance.

## 6. Conclusion

This framework provides a structured approach to data management, ensuring security, compliance, and efficient handling of organizational data. Regular reviews will be conducted to adapt to evolving regulations.

📌 Next Steps: Implement governance tools for automated policy enforcement. 🚀