# Data Governance Framework

## 1. Overview

This document outlines the Data Governance Framework, which includes governance structure, data classification, and data lifecycle management policies. This is classified as an advanced level of data governance maturity.

## 2. Governance Structure

### Data Ownership Roles

* **Chief Data Officer**: Oversees overall data governance strategy and execution.
* **Chief Information Security Officer**: Ensures security controls and data protection compliance.
* **Compliance Manager**: Monitors regulatory compliance and policy adherence.
* **Data Stewards**: Responsible for managing and ensuring the quality, integrity, and security of data within specific domains.

## 3. Data Classification

|  |  |
| --- | --- |
| **Classification** | **Description** |
| 1. Public Data | * Non-sensitive information, available for public access without restrictions. |
| 2. Internal Data | * Restricted to organizational use only; not intended for public distribution. |
| 3. Confidential Data | * Includes customer financial data; access restricted to authorized personnel. |
| 4. Highly Sensitive Data | * Includes personal identification details and transactional information; the highest level of protection required. |

## 4. Data Lifecycle Management

### A. Creation

• Implementation of validated input mechanisms to ensure data accuracy and consistency during capture.

### B. Storage

• All sensitive data is to be encrypted.

• Data must be stored in segregated environments based on classification level.

### C. Access

• Controlled through Strict Role-Based Access Control.

• Access is granted based on job responsibilities and data classification.

### D. Retention

• Transaction Records: Retained for 7 years.

• Customer Records: Retained for 10 years post account closure.

• Loan Documents: Retained for the life of the loan, 7+ years.