**Data Governance Document**

**1. Governance Structure**

Data governance ensures that data is properly managed, secured, and utilized effectively within the organization. The governance structure consists of the following key roles:

* **Chief Data Officer (CDO):** Responsible for overall data strategy, management, and governance policies.
* **Chief Information Security Officer (CISO):** Ensures data security, compliance with regulations, and mitigates cybersecurity risks.
* **Compliance Manager:** Oversees adherence to regulatory requirements and data governance policies.
* **Data Stewards:** Assigned for each domain to ensure data quality, integrity, and security.

**2. Data Classification**

Data is categorized into four levels based on its sensitivity and required security measures:

1. **Public Data:** Non-sensitive information that can be freely shared (e.g., marketing materials, website content).
2. **Internal Data:** Restricted to organizational use only (e.g., internal reports, business strategies).
3. **Confidential Data:** Includes customer financial information, trade secrets, and internal analytics that require controlled access.
4. **Highly Sensitive Data:** Includes personal identification details, transaction records, and legally protected information that require the highest level of security.

**3. Data Lifecycle Management**

Effective data lifecycle management ensures data integrity, security, and compliance throughout its lifecycle:

**3.1 Data Creation**

* Data input mechanisms must be validated to prevent inaccuracies.
* Standardized formats and metadata tagging should be implemented.

**3.2 Data Storage**

* All sensitive data must be encrypted and stored in segregated databases.
* Secure backup procedures must be followed to prevent data loss.

**3.3 Data Access**

* Strict **Role-Based Access Control (RBAC)** ensures only authorized personnel access specific data categories.
* Multi-factor authentication (MFA) should be enforced for accessing confidential and highly sensitive data.

**3.4 Data Retention**

* **Transaction records:** Retained for **7 years** as per financial regulations.
* **Customer records:** Retained for **10 years post-account closure** for compliance and audit purposes.
* **Loan documents:** Retained for **the life of the loan + 7 years** to meet legal and financial requirements.

**Conclusion**

This Data Governance Document establishes a structured approach to managing data within the organization. By enforcing clear governance roles, classification levels, and lifecycle policies, we ensure compliance, security, and operational efficiency in handling critical data assets.