Title: Data Governance Policies of Bank DEF

1. Introduction

1.1 Purpose

This document outlines the data governance policies at Bank DEF. It serves as a framework for managing data quality, security, and compliance across the organization.

1.2 Scope

The policies in this document apply to all employees, contractors, and third-party partners handling data at Bank DEF.

1.3 Definitions

- **Data Governance**: The framework for ensuring data accuracy, availability, and security.
- **Data Steward**: An individual or team responsible for overseeing data management practices and ensuring compliance with policies.

2. Data Governance Framework

2.1 Governance Structure

The governance structure at Bank DEF ensures effective data management and accountability:

Role	Description
Data Governance Board	**Responsible for strategic oversight and policy approval.**
Data Stewards	**Manage and monitor data quality and adherence to policies.**
Data Custodians	**Implement and enforce data management practices and security measures.**

2.2 Responsibilities

- **Data Governance Board**: Develops data management strategy, approves policies, and ensures alignment with business goals.
- **Data Stewards**: Oversee data quality, address data issues, and support policy implementation.

- **Data Custodians**: Manage daily data operations, including security and compliance.

3. Data Quality Management

3.1 Data Quality Standards

Maintaining high data quality is essential. The standards include:

Standard	Description
Accuracy	Data must be accurate and free from errors.
Completeness	All required data fields must be filled.
Consistency	Data should be consistent across systems and sources.

3.2 Data Quality Metrics

Metrics used to measure data quality:

Metric	Definition	Target Value
Error Rate	Percentage of data entries with errors	< 2%
Completeness Score	Percentage of data fields completed	100%
Consistency Rate	Percentage of consistent data across systems	> 95%

4. Data Security and Privacy

4.1 Data Classification

Data is classified to ensure appropriate protection:

Classification	Description
Confidential	**Highly sensitive data (e.g., customer financial records).**
Internal Use Only	**Data restricted to internal use (e.g., employee records).**
Public	**Data that can be shared externally (e.g., quarterly reports).**

4.2 Access Controls

Access to data is managed through:

Control Method	Description
Role-Based Access Control (RBAC)	**Permissions based on user roles and responsibilities.**
Multi-Factor Authentication (MFA)	**Additional security for accessing sensitive data.**

5. Data Handling Procedures

5.1 Data Entry and Validation

Procedures for data entry and validation:

- **Data Entry**: Guidelines for entering data accurately.
- **Validation**: Rules for verifying data accuracy and completeness.

5.2 Data Retention and Disposal

Data retention and disposal policies:

Data Type	Retention Period	Disposal Method
Customer Data	6 years	Secure Deletion
Employee Records	4 years after termination	Secure Deletion
Transaction Data	8 years	Archival Storage

6. Data Policies

6.1 Policy Overview

Data governance policies provide guidelines for managing and protecting data. Each policy is identified by a unique PolicyID and includes detailed PolicyInformation.

6.2 Data Policies Table

PolicyID	PolicyTitle	PolicyInformation
001	Data Accuracy Policy	Ensures all data entered into systems is accurate and free from errors.
002	Data Retention Policy	Defines how long different types of data should be retained and the methods for disposal.
003	Data Access Control Policy	Outlines the methods and procedures for controlling access to data based on user roles and responsibilities.
004	Data Classification Policy	Provides guidelines for classifying data into categories to apply appropriate security measures.
005	Data Security Policy	Establishes procedures for protecting data from unauthorized access and breaches.
006	Data Quality Management Policy	Describes the procedures for monitoring and maintaining data quality.

7. Compliance and Audits

7.1 Regulatory Compliance

Compliance with key regulations:

Regulation	Description
GDPR	**General Data Protection Regulation compliance.**
SOX	**Sarbanes-Oxley Act compliance (financial data).**

7.2 Internal Audits

The audit process includes:

Audit Aspect	Description
Audit Frequency	**Semi-annual or as needed.**
Audit Findings	**Includes non-compliance issues and corrective actions.**

8. Training and Awareness

8.1 Training Programs

Training programs for data governance:

Program	Description
Data Governance Training	**Regular training on data governance policies and best practices.**
Compliance Training	**Training on specific compliance requirements and regulations.**

8.2 Awareness Campaigns

Ongoing awareness strategies:

Campaign	Description
Policy Reminders	Regular reminders about data governance policies.
Support Resources	Resources available for questions about data policies.

9. Contact Information

9.1 Data Governance Team

For inquiries related to data governance:

Name	Role	Email
Alice Johnson	Chief Data Officer	alice.johnson@bankdef.com
Bob Brown	Data Governance Analyst	bob.brown@bankdef.com