

**Title: Data Governance Policies of Bank DEF (Supplemental Data)**

**1. Introduction**

**1.1 Purpose**

This document provides supplemental data related to the data governance policies of Bank DEF. It includes additional details on data classifications, security controls, and compliance measures that complement the primary governance framework.

**1.2 Scope**

The data in this document supports the policies outlined in Document A and is relevant to all employees, contractors, and third-party partners handling data at Bank DEF.

**1.3 Definitions**

- **Data Custodian:** The individual responsible for managing and safeguarding data assets.
- **Compliance Officer:** An individual responsible for ensuring adherence to regulatory requirements and internal policies.

**2. Data Classification and Security**

**2.1 Data Classification Details**

Data is classified to apply appropriate handling and protection measures. The following details provide additional context:

| Classification    | Example Data Types                          | Security Measures                             |
|-------------------|---|---|
| Confidential      | Customer account details, credit histories  | Encryption, restricted access, audit trails   |
| Internal Use Only | Employee contact lists, internal memos      | Password protection, internal access controls |
| Public            | Press releases, general financial summaries | Minimal security, open access                 |

**2.2 Security Controls**

Specific security measures are applied to each data classification:

| Data Classification | Control Measure | Description   |
|---------------------|-----------------|---|
| Confidential        | Data Encryption | Encrypts sensitive data to prevent unauthorized access. |
| Internal Use Only   | Access Logs     | Maintains logs of who accessed the data and when.       |
| Public              | Data Masking    | Masks sensitive portions of data shared publicly.       |

### 3. Data Management Procedures

#### 3.1 Data Entry Standards

Standards for data entry ensure consistency and accuracy:

| Standard         | Description  |
|------------------|--|
| Data Format      | Standardize formats for dates, numbers, etc.       |
| Validation Rules | Rules for checking data accuracy and completeness. |

#### 3.2 Data Quality Assurance

Procedures for ensuring ongoing data quality:

| Procedure       | Description   |
|-----------------|---|
| Data Audits     | Regular audits to verify data quality and compliance. |
| Data Correction | Processes for correcting identified data issues.      |

## 4. Compliance and Audit Procedures

### 4.1 Compliance Requirements

Additional compliance measures and regulations:

| Regulation | Requirement              | Description  |
|------------|--------------------------|--|
| GDPR       | Data Subject Rights      | Ensure processes for data subject access requests.           |
| SOX        | Financial Data Integrity | Maintain controls for financial data accuracy and reporting. |

### 4.2 Audit Process

The audit process for data governance compliance:

| Audit Type      | Frequency     | Description  |
|-----------------|---------------|--|
| Internal Audits | Semi-annually | Regular reviews to ensure adherence to policies and regulations.   |
| External Audits | Annually      | Third-party audits to validate compliance with industry standards. |

## 5. Data Access and Management

### 5.1 Data Access Procedures

Access procedures to ensure proper data management:

| Procedure       | Description  |
|-----------------|--|
| Access Requests | Process for requesting access to data.                           |
| Access Reviews  | Regular reviews of access permissions to ensure appropriateness. |

### 5.2 Data Management Best Practices

Best practices for managing data:

| Practice              | Description                                     |
|-----------------------|---|
| Regular Backups       | Regular backups to prevent data loss.           |
| Data Integrity Checks | Checks to ensure data is accurate and reliable. |

## 6. Training and Awareness

### 6.1 Additional Training Programs

Supplementary training programs for employees:

| Program                | Description  |
|------------------------|--|
| Advanced Data Security | In-depth training on advanced security measures and data protection. |
| Compliance Workshops   | Workshops focused on specific compliance requirements and updates.   |

6.2 Awareness Strategies

Strategies to enhance awareness of data governance policies:

| Strategy             | Description   |
|----------------------|---|
| Regular Updates      | Periodic updates on policy changes and data governance issues.              |
| Interactive Sessions | Interactive sessions for employees to engage with data governance concepts. |

7. Contact Information

7.1 Compliance and Data Management Team

For additional queries related to compliance and data management:

| Name        | Role               | Email  |
|-------------|--------------------|--|
| David Green | Compliance Officer | <a href="mailto:david.green@bankdef.com">david.green@bankdef.com</a> |
| Linda Brown | Data Custodian     | <a href="mailto:linda.brown@bankdef.com">linda.brown@bankdef.com</a> |