DATA INTEGRITY POLICY

1. Purpose

The purpose of this policy is to establish guidelines for ensuring the integrity, accuracy, and reliability of data within the organization. Maintaining data integrity is critical to supporting business operations, compliance requirements, and decision-making processes.

1. Scope

This policy applies to all employees, contractors, and third-party service providers who handle, process, or store organizational data. It covers all data types, including structured and unstructured data, across all information systems and platforms.

1. Data Integrity Principles

To uphold data integrity, the organization will adhere to the following principles:

* Accuracy: Ensuring data is correct, consistent, and updated in a timely manner.
* Consistency: Maintaining uniformity and reliability across all data sources and platforms.
* Completeness: Ensuring all necessary data is captured and retained without omission.
* Security: Protecting data from unauthorized access, corruption, or loss.
* Auditability: Implementing mechanisms to track and verify data changes.

4. Roles and Responsibilities

* GRC Analyst: Oversees policy enforcement, compliance, and risk assessments related to data

integrity.

* IT and Security Teams: Implement technical controls to maintain data accuracy and protect against breaches.
* Data Owners: Ensure data within their domain is accurate, complete, and compliant with organizational policies.
* All Employees: Responsible for adhering to data integrity protocols and reporting discrepancies.

5. Data Integrity Controls

* Access Control: Implement role-based access controls (RBAC) to restrict unauthorized data modifications.
* Data Validation: Use automated validation checks to prevent input errors and inconsistencies.
* Change Management: Require proper authorization and documentation for all data modifications.
* Backup and Recovery: Establish regular data backups and recovery plans to prevent data loss.
* Audit Logging: Maintain detailed logs of data access and changes for monitoring and compliance purposes.

1. Compliance and Monitoring

* Regular audits and monitoring will be conducted to ensure adherence to this policy. Any violations or discrepancies will be addressed through corrective actions, which may include additional training, process improvements, or disciplinary measures.

1. Policy Review and Updates

* This policy will be reviewed annually or as needed to align with evolving regulatory requirements and organizational needs. Any updates will be communicated to all relevant stakeholders.

1. Enforcement

* Non-compliance with this policy may result in disciplinary action, including suspension of system access, termination of employment, or legal action as deemed necessary.

Approval and Acknowledgment

By signing below, I acknowledge that I have read, understood, and agree to comply with the Data Integrity Policy.

Employee Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_