

# FutureMart Data Governance Plan

## 1. Purpose and Scope

### Purpose:

The data governance plan at FutureMart aims to ensure data integrity, privacy, security, and effective use across the organization. It supports compliance with legal regulations and empowers data-driven decision-making.

### Scope:

This governance plan applies to all business areas including sales, marketing, customer service, inventory management, and finance, covering all types of data generated, stored, and processed.

## 2. Data Governance Objectives

- **Data Quality:** Ensure data is accurate, complete, consistent, and timely.
- **Data Security:** Protect sensitive and personal data against unauthorized access.
- **Data Compliance:** Adhere to all applicable laws and regulations such as GDPR, HIPAA, or local data protection acts.
- **Data Availability:** Ensure authorized users have reliable and timely access to data.
- **Data Consistency:** Maintain uniformity of data across systems and platforms.
- **Data Usage:** Promote responsible use of data to support business insights and operations.

## 3. Data Governance Framework

- **Data Governance Steering Committee:** Sets strategy and policies, oversees compliance.
- **Data Stewards:** Manage day-to-day data quality and policy enforcement within departments.
- **Data Owners:** Responsible for data accuracy and usage permissions.
- **Data Users:** Access and utilize data responsibly, following policies.

### Key Policies:

- **Data Collection Policy:** Data must be collected transparently, with consent, and stored securely.
- **Data Usage Policy:** Data is used only for approved business purposes, respecting privacy.
- **Data Retention Policy:** Data is retained based on regulatory requirements and business needs; secure archival and deletion are enforced.
- **Data Privacy & Security Policy:** Data encryption, masking, and strict access controls are mandatory.

## 4. Data Management Practices

- **Data Classification:** Data is categorized as Public, Internal, Confidential, or Restricted.
- **Data Quality Management:** Implement validation rules and periodic audits to maintain accuracy.
- **Data Integration:** Use standardized protocols and ETL processes for consistent data flow.
- **Data Documentation:** Maintain comprehensive metadata and data lineage documentation.

## 5. Data Security and Privacy Policies

- **Encryption & Masking:** Encrypt data at rest and in transit; mask sensitive fields where necessary.
- **Access Control:** Role-based access controls limit data access to authorized personnel only.
- **Incident Management:** Establish clear procedures to detect, report, and respond to data breaches.

## 6. Compliance and Legal Considerations

- **Regulatory Compliance:** FutureMart complies with GDPR, local data protection laws, and industry standards.
- **Data Auditing & Reporting:** Regular audits are conducted; compliance reports are generated for stakeholders.
- **Data Retention & Disposal:** Data retention periods comply with laws; secure destruction of obsolete data is enforced.

## 7. Additional Components (Optional)

- **Governance Tools:** Utilize data management platforms such as Collibra or Informatica.
- **Training & Awareness:** Regular staff training on data governance policies and security best practices.
- **Performance Metrics:** KPIs to monitor data quality, security incidents, and compliance adherence.
- **Implementation Plan:** Phased rollout with resource allocation, continuous monitoring, and improvement cycles.