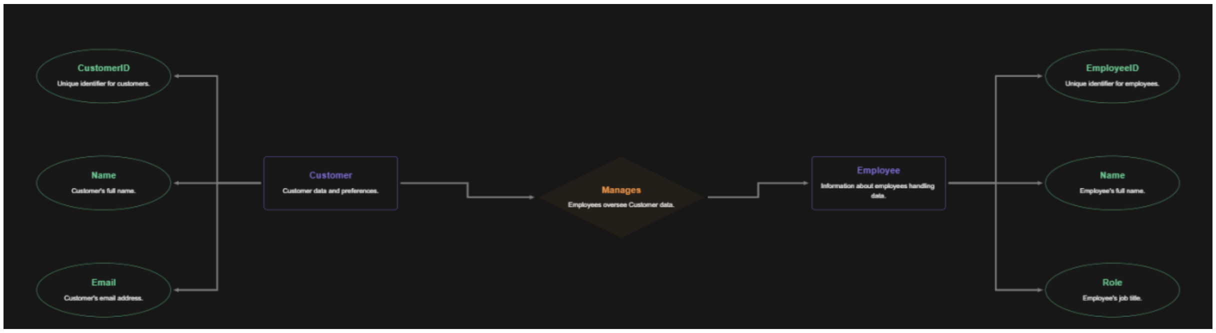
Purpose & Scope:
Ensure data accuracy, security, privacy, and regulatory compliance across all FutureMart operations (sales, marketing, inventory, finance).
Objectives:
Maintain high data quality standards.
Protect customer and employee data via encryption and access controls.
Comply with GDPR, CCPA, and other relevant laws.
Ensure data availability for authorized users.
Promote consistent data definitions and usage.
Data Management Practices:
Classify data as public, internal, confidential, restricted.
Implement validation, cleansing, and regular audits.
Standardize data integration methods.
Document data models and flows.
Security & Privacy Policies:
Encrypt data at rest and transit.
Limit access based on roles.
Monitor and respond to security incidents promptly.
Compliance & Legal Considerations:
Adhere to GDPR, CCPA, HIPAA (if applicable).
Conduct quarterly audits.
Establish data retention timelines and secure disposal procedures.


CustomerID
Unique identifier for customers.
Name
Customer's full name.
Email
Customer's email address.
Customer
Customer data and preferences.
Manages
Employees oversee Customer data.
Employee
Information about employees handling data.
EmployeeID
Unique identifier for employees.
Name
Employee's full name.
Role
Employee's job title.

This ensures that data is:

- Accurate
- Secure
- Consistent
- Compliant with laws
- Accessible for authorized users

This plan aims to **maximize the value of data** while **minimizing risks** like breaches, inaccuracies, or non-compliance.

Scope of the Plan

The scope defines **which parts of the organization and data** are covered:

- **Customer Data:** Personal info, purchase history, preferences
- **Sales & Marketing Data:** Campaigns, lead info, engagement metrics
- **Inventory & Supply Chain Data:** Stock levels, logistics, supplier info
- **Financial Data:** Payments, invoices, financial reports

- **Employee Data:** HR records, payroll, access credentials

Operational coverage includes:

- All digital and physical channels (online store, physical stores, warehouses)
- All departments involved in handling and processing data
- Data lifecycle stages (creation, storage, usage, sharing, archiving, disposal)

2. Objectives of Data Governance

Set clear objectives aligned with business goals:

Data Quality

- Ensure data is complete, accurate, and up-to-date.
- Regularly audit and cleanse data to prevent errors.

Data Security

- Protect sensitive customer and business data from unauthorized access.
- Use encryption, access controls, and secure protocols.

Data Compliance

- Adhere to relevant laws/regulations like GDPR, CCPA, PCI-DSS, etc.
- Maintain audit trails for compliance reporting.

Data Availability

- Ensure that authorized personnel can access necessary data promptly.
- Minimize downtime and data access restrictions.

Data Consistency

- Use standardized data definitions and formats across all systems.
- Prevent discrepancies between systems or departments.

Data Usage

- Facilitate informed decision-making through accessible, reliable data.
- Support analytics, AI, and reporting initiatives.

Data Governance Framework

Roles & Responsibilities

- **Data Governance Steering Committee:**
  Senior executives, legal, compliance officers overseeing overall governance, policy approval, and strategic direction.

- **Data Stewards:**
  Responsible for data quality, standards, and lifecycle management within specific domains (Customer Data, Inventory Data).

- **Data Owners:**
  Department heads responsible for data accuracy, security, and compliance within their datasets.

- **Data Users:**

Employees and analysts who access and use data for operational or analytical purposes.

Policies & Standards

- **Data Collection Policy:**
    - Define how customer data is captured (online forms, in-store sign-ups).
    - Ensure consent and legal compliance.
    - Use secure methods for data transfer and storage.
- **Data Usage Policy:**
    - Limit data access based on roles.
    - Prohibit misuse or unauthorized sharing.
    - Support ethical data practices.
- **Data Retention Policy:**
    - Define how long data is kept (customer data retained for 5 years).
    - Specify procedures for archiving or deleting outdated data.
- **Data Privacy & Security Policy:**
    - Encrypt sensitive data in storage and transit.
    - Mask or anonymize data where necessary.
    - Control access with authentication and authorization.

4. Data Management Practices

Data Classification

- **Public Data:** Publicly available info (marketing materials).
- **Internal Data:** Operational data accessible within the company (employee directories).
- **Confidential Data:** Customer info, financial data, trade secrets.
- **Restricted Data:** Highly sensitive data, e.g., payment details, health info.

Handling:

- Public: No restrictions.
- Confidential/Restricted: Encrypted, limited access, monitored.

Data Quality Management

- Regular validation and cleansing processes.
- Use automated tools for deduplication and consistency checks.
- Maintain metadata and data dictionaries.

Data Integration Practices

- Standardize data formats and protocols (APIs, ETL pipelines).
- Use master data management (MDM).
- Document data lineage.

Data Documentation

- Maintain data dictionaries, schemas, and flow diagrams.
- Document data sources, transformation rules, and access rights.

Data Security & Privacy Policies

- **Encryption & Masking:**
  - Encrypt data at rest using AES-256 or similar.
  - Mask sensitive info on screens or reports.
- **Access Control Policy:**
  - Role-based access controls (RBAC).
  - Multi-factor authentication (MFA).
  - Regular review of permissions.
- **Incident Management:**
  - Procedures for detecting, reporting, and responding to data breaches.
  - Notification timelines aligned with regulations.
  - **Compliance & Legal Policies**
- **Regulatory Requirements:**
  - **GDPR:** Data subject rights, consent, right to be forgotten.
  - **CCPA:** Opt-out rights, data access rights.
  - **PCI-DSS:** Payment data security.
  - **HIPAA (if applicable):** Patient data regulations.
- **Auditing & Reporting:**
  - Regular internal audits of data handling.
  - Maintain logs for data access and modifications.
  - Prepare compliance reports quarterly or annually.
- **Data Retention & Disposal:**
  - Define retention periods per data type.
  - Secure deletion procedures (overwriting, shredding).
  - Document disposal actions.
- **Tools & Technologies:**
  - Data governance platforms (Collibra, Informatica).
  - Data catalog and lineage tools.
  - Monitoring dashboards.
- **Training & Awareness:**
  - Regular training sessions for staff on data policies.
  - Awareness campaigns on data security best practices.
- **Performance Metrics:**
  - Data quality scores.
  - Number of security incidents.
  - Compliance audit results.
- **Implementation Plan:**
  - Phased rollout.
  - Assigning roles and responsibilities.
  - Continuous monitoring and updates