Data Governance Policy Template

Customizable data governance policy template for roles, access, and compliance. Covers 5 core policy areas and review cadence.

EN · document · governance

Template Overview This template provides a structured framework for creating data governance policies. It includes all essential sections with guidance on what to include and how to customize for your organization's needs. Use this template as a starting point and adapt the content to reflect your specific: • Organizational structure • Regulatory requirements • Industry standards • Data landscape How to Use This Template • Copy the template to your preferred document format • Replace bracketed text with your organization's specifics • Review with stakeholders including legal, compliance, IT, and business • Obtain approval from your data governance council • Publish and communicate to all relevant employees • Schedule regular reviews (recommended: annually) Template Content --- [Organization Name] Data Governance Policy Version: [X.X] Effective Date: [Date] Last Reviewed: [Date] Policy Owner: [Role/Name] Approved By: [Data Governance Council / Executive] --- • Purpose This policy establishes the framework for governing data across [Organization Name]. It defines roles, responsibilities, and standards to ensure data is managed as a strategic asset while maintaining quality, security, and compliance. 1.1 Objectives This policy aims to: • Establish clear accountability for data assets • Ensure data quality meets business requirements • Protect sensitive data from unauthorized access • Enable compliant use of data across the organization • Support data-driven decision making --- • Scope 2.1 Data Coverage This policy applies to: • All data created, collected, processed, or stored by [Organization Name] • Data in all formats: structured, unstructured, and semi-structured • Data in all locations: on-premises, cloud, third-party systems 2.2 Organizational Coverage This policy applies to: • All employees of [Organization Name] • Contractors and consultants with data access • Third-party vendors processing our data • [Add other applicable groups] 2.3 Exclusions This policy does not cover: • [List any explicit exclusions] --- • Definitions | Term | Definition | |------|-----------| | Data Asset | Any collection of data that has value to the organization | | Data Domain | A logical grouping of related data (e.g., Customer, Product, Financial) | | Data Owner | Business executive accountable for a data domain | | Data Steward | Individual responsible for day-to-day data management | | Data Custodian | Technical role responsible for data storage and security | | Metadata | Data that describes other data (definitions, lineage, quality rules) | | PII | Personally Identifiable Information | | [Add organization-specific terms] | [Definitions] | --- • Governance Structure 4.1 Data Governance Council Purpose: Provide strategic oversight for data governance initiatives. Composition: • Chief Data Officer (Chair) • [List other members/roles] Responsibilities: • Set data governance strategy and priorities • Approve data policies and standards • Resolve cross-domain data issues • Allocate resources for data initiatives Meeting Cadence: [Monthly/Quarterly] 4.2 Data Owners Responsibilities: • [ ] Define business requirements for data in their domain • [ ] Approve data access requests • [ ] Ensure compliance with data policies • [ ] Assign data stewards • [ ] Escalate unresolved issues to the governance council 4.3 Data Stewards Responsibilities: • [ ] Maintain data quality within their domain • [ ] Document business metadata and data definitions • [ ] Implement data governance policies • [ ] Provide training and support to data users • [ ] Report on data quality metrics 4.4 Data Custodians Responsibilities: • [ ] Implement technical security controls • [ ] Manage data storage and backup • [ ] Execute data retention and archival procedures • [ ] Support data access provisioning • [ ] Maintain technical metadata --- • Data Classification All data assets must be classified according to the following scheme: 5.1 Classification Levels | Level | Description | Examples | Handling Requirements | |-------|-------------|----------|----------------------| | Public | No restrictions on disclosure | Marketing materials, public website | Standard controls | | Internal | For internal use only | Internal reports, org charts | Access logging | | Confidential | Sensitive business information | Financial data, strategies | Encryption, need-to-know access | | Restricted | Highest sensitivity | PII, PHI, trade secrets | Encryption, MFA, audit trail | 5.2