Data Governance Policy Template

By Paul Kirvan, FBCI, CISA

Title: Data Governance Policy	
Department:	**Version:** Original
Approved by:	**Approval Date:**
Senior Management Approval:	
Effective Date:	**Last Updated:**
Author:	

Scope

This policy applies to the <specify location> of <company name>

<enter address>

Authority

This policy is hereby approved and authorized.

__________________________ ______________________________ _____________
Signature Title Date

__________________________ ______________________________ _____________
Signature Title Date

Purpose

The purpose of this policy is to define data governance activities associated with the development, updating, deployment and management of data quality, data access, data security, data usage and data privacy activities within <company name>. Additional policies governing data management activities will be addressed separately.

Additional purposes for this plan include compliance with applicable standards and regulations governing data governance, and compliance with environment, sustainability and related regulations.

Scope

The scope of this data governance policy is the data generated by <company name>, and includes all information technology systems, software, databases, and applications needed by the Company to conduct its business. The policy is applicable to all Company employees, contractors and other authorized third-party organizations.

Statement of Compliance

This policy is designed to be compliant with the U.S. Data Protection Act of 1998; Freedom of Information Act of 2000; Fair and Accurate Credit Transactions Act of 2003 (FACTA); Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada; Gramm-Leach-Bliley Act (GLBA); the European Union General Data Protection Regulation (GDPR); California Consumer Privacy Act (CCPA); ISO 27040, Information Technology, Security Techniques, Storage Security; and NIST SP 800-209, Security Guidelines for Storage Infrastructure.

The Information Technology (IT) department manages data governance policy with support from <company name> department leadership and subject matter experts (SME). To meet compliance requirements, data governance programs must include appropriate procedures and identify staffing and technology resources. The IT department, internal audit or other appropriate entities verify compliance monthly.

Policy

The IT department is responsible for managing all data governance activities for the Company. Other departments, such as Finance and Accounting, Operations and Human Resources, are responsible for providing the IT department with their requirements for data quality, privacy, security and usage.

The IT department is responsible for developing, executing and periodically testing data governance procedures and, in its activities, ensuring compliance with appropriate industry standards for data governance.

1. The company shall develop comprehensive data governance plans in accordance with good data governance practices as defined by established standards.
2. Data governance activities shall be supported by the company's data management program, which administers and manages the overall technology data management program that encompasses:
   - Planning and design of data quality, security, privacy usage and access activities;
   - Identification of data governance teams, including data stewards, and data architects and engineers, defining their roles and responsibilities and ensuring they are properly trained and prepared to perform their duties;
   - Planning, design and documentation of data quality, security, privacy, usage and related governance plans;
   - Scheduling of updates to risk assessments associated with data governance;
   - Planning and delivery of awareness and training activities for employees and data governance team members;
   - Planning and execution of data governance exercises;

- Designing and implementing data governance maintenance activities to ensure plans are up to date and ready for use;
  - Ensuring that data governance procedures are consistent with the Company's environmental and sustainability management programs;
  - Preparing for management review and auditing of data governance plan(s); and
  - Planning and implementation of continuous improvement activities for data governance activities and plans.

3. Formal risk assessments (RA) and business impact analyses (BIA) shall consider the inclusion of data governance activities; RAs and BIAs shall be updated at least annually to ensure alignment with data governance policy requirements.
4. Data governance plans, such as those addressing data quality and data ownership, shall address electronic data stored on electronic media such as CDs, hard disk drives, solid-state disk drives, magnetic tape and other approved media.
5. Data governance plans, such as those addressing data quality and data ownership, shall address data stored on non-electronic media (e.g., paper files, microfiche).
6. Data governance plans shall facilitate establishing the data quality requirements and associated metrics for electronic and non-electronic information and systems supporting the IT infrastructure.
7. Data governance and associated plans and schedules shall be periodically reviewed and tested in a suitable environment to ensure that data quality and related issues associated with databases, media, systems, and other relevant elements can be validated and that <company name> management and employees understand how the plans and schedules are to be executed as well as their roles and responsibilities.
8. Data governance and related plans and schedules will be consistent with environmental and sustainability programs the Company has established.
9. All employees must be made aware of the data governance program and their own roles and responsibilities
10. Data governance and associated plans and other documents are to be kept up to date and will reflect existing and changing circumstances.

Data Governance Specifications

Following are specific data governance requirements:

General

1. State the frequency and types of data governance activities to be performed.
2. State the frequency and types of data quality activities to be performed.
3. State the schedule for data governance and related activities..
4. State who (e.g., internal staff, outside third parties) is responsible for data governance.
5. State who should be notified if a problem with data governance and related activities is identified.

Data Quality Procedures

1. State how data (e.g., electronic and non-electronic) is stored and retained.

2. State how data quality is monitored.
3. State the schedule for data quality activities.
4. State the process for ensuring that data quality procedures work properly.
5. State the process for validation of data/media quality.
6. State process for complying with Company environmental and sustainability programs.

Data Security and Privacy

1. State process for access controls and authentication.
2. State policy on data encryption (e.g., at rest and in motion).
3. State policy on ensuring data privacy.
4. State process for auditing data security and privacy activities.

Data Ownership and Responsibility

1. State the process for defining data ownership.
2. State the process for identifying data owners and stewards.
3. State responsible parties for data governance leadership.
4. State how data governance is a part of <company name> business culture.

Data Governance Performance Metrics

1. State how data governance initiatives are to be monitored and assessed.
2. State key performance indicators (KPI) and other metrics that will be used to measure data governance, data quality, data ownership and related activities.
3. State the tools to monitor data governance activities, such as dashboards and third-party software

Policy Leadership

<Title of executive> is designated as the corporate owner responsible for data governance activities for the Company. Resolution of issues in the support of data governance activities should be coordinated with IT management and others as needed.

Policy Responsibilities

- Policy Approval – The **<title of executive>** is responsible for approving this policy.
- Policy Implementation – The <enter name of department or individual> is responsible for planning, organizing and implementing all activities that fulfill this policy.
- Policy Maintenance and Updating – The <enter name of department or individual> is responsible for all activities associated with maintaining and updating this policy.
- Policy Compliance – The <enter name of department or individual> is responsible for ensuring compliance with relevant standards, regulations and good practice for data governance, data quality and related activities
- Policy Compliance with Environment Management Programs – The <enter name of department or individual> is responsible for ensuring compliance with Company policies

and programs for environment and sustainability management

- Policy Monitoring, Review and Audit – The <enter name of department or individual> is responsible for monitoring and reviewing this policy and providing support for scheduled audits – both internally and externally executed – on data governance and related activities.
- Policy Improvement – The <enter name of department or individual> is responsible for defining and implementing activities that will improve this policy.

Management Review

<Enter name of department or individual> will review and update this data governance policy annually. As changes to this policy are needed in the course of business, <enter name of department or individual> may initiate a change management process to update this policy.

Policy Enforcement

The **<title of executive>** will enforce this policy.

Penalties for Non-Compliance

In situations where it is determined that data governance and related activities do not comply with this policy, the IT department team assigned to this activity will prepare a report stating the reason(s) for non-compliance and present it to IT management for resolution. Failure to comply with this data governance policy within the allotted time for resolution may result in consequences ranging from verbal reprimands, notes in personnel files, termination, and such other remedies as deemed appropriate.

Policy Location

The policy will be signed, scanned into an electronic file and posted in the following location on the network: <enter location of policy>