**Data Stewardship Policy Sample**

# Purpose

# The purpose of this Data Stewardship Policy is to establish guidelines and responsibilities for managing, protecting, and using data within [Agency]. This policy aims to ensure data integrity, confidentiality, and availability while promoting effective data management practices.

# Scope

This policy applies to all employees, contractors, and third-party agents who handle, manage, or use data owned by or entrusted to [Agency].

# Definitions

| **Term** | **Definition** |
| --- | --- |
| **Business Glossary** | A centralized repository of definitions and business terms used within the organization to ensure consistent understanding and usage of terminology. |
| **Metadata** | Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. |
| **Metadata standards** | Guidelines and specifications for creating, managing, and maintaining metadata |
| **NIEM Core** | A framework designed to facilitate the exchange of information across different domains, such as justice, public safety, emergency management, and health which is part of the National Information Exchange Model (NIEM). |
| **Data Owner** | The person or entity responsible for the overall data governance of a dataset, typically a senior leader within the organization. |
| **Data Steward** | An individual responsible for managing a dataset and ensuring its quality and metadata accuracy. |
| **Data User** | Any individual who interacts with data for analysis, reporting, or operational purposes. |
| **Data Custodian** | IT personnel responsible for the technical environment and security where data is stored, processed, and transmitted. |
| **ISO** | Information Security Officer is responsible for developing and managing the agency’s information security program. |
| **Critical Data Asset** | Any data asset determined to be critical to the mission of one or more COV agencies as determined by the agency designated Data Owner or Data Steward. |

# Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| **Data Steward** | * Ensure data accuracy, completeness, and consistency. * Monitor data usage and compliance with policies and regulations. * Maintain metadata and data documentation. * Facilitate data quality assessments and improvements. * Manage and update the business glossary to ensure it reflects current terminology and definitions. |
| **Data Owner** | * Define data governance policies and procedures. * Approve access to data and determine data classification levels. * Ensure compliance with legal, regulatory, and organizational requirements. |
| **Data User** | * Use data responsibly and ethically. * Protect sensitive data and report any breaches or suspicious activities. * Assess and monitor data quality. * Act as advocates for Data Governance within their organization. * Classify and prioritize data based on the sensitivity and criticality. * Adhere to data usage guidelines and security policies. |
| **Data Custodians** | * Implement and maintain technical safeguards to protect data. * Ensure data backup, recovery, and disaster recovery procedures are in place. * Manage access controls and monitor data system security. |

# Policy

All [AGENCY] employees must adhere to the following data stewardship policies when creating, managing, or using data.

* The Data Steward at each agency must maintain a comprehensive data inventory that lists all data assets under its control, including data sets, databases, files, and data sources as described in the [COV Data Governance Policy].
* For all critical data assets, Data Owners must assign a data steward who is responsible for the asset’s quality, security and compliance.
* The Data Steward must ensure data is accurate, complete, timely, and consistent as described in the [COV Data Quality Policy].
* Data Stewards must maintain the quality of the data using customer feedback, concerns, internal reporting metrics, evaluating and identifying the issues, finally coordinating and implementing those corrections.
* Data stewards must ensure data is used for its intended purposes and enforce compliance with applicable regulations.
* The Data Steward and Data Custodian must implement measures to protect data from unauthorized access, alteration, or destruction as described in the [COV Data Security Policy].
* The Data Owner, Steward and Users must handle personal data in compliance with applicable privacy laws and regulations as described in the [COV Data Privacy Policy].
* The Data Custodian must ensure data is available to authorized users when needed, while protecting it from unauthorized access.
  + Access to data should be granted based on the principle of least privilege.
  + Data users must follow access approval processes defined by data owners.
  + Data usage should comply with all relevant policies, laws, and regulations.
* The Data Steward must manage data from creation to disposal, ensuring proper archival and destruction of data when no longer needed as described in the [COV Data Retention Policy] and in compliance with the Library of Virginia’s Retention Policy.
* The Data Steward must maintain up-to-date metadata to provide context, improve data usability, and support data governance activities as described in the [COV Metadata Management Policy]
* The Data Steward must regularly update the business glossary to ensure clarity, consistency, and alignment with organizational terminology.
* The Data Steward must ensure data exchanges and integrations align with NIEM standards to facilitate interoperability and information sharing across different systems and organizations as described in the [COV Metadata Management Policy].
* The Data Steward and Data Users must ensure data is classified based on its sensitivity and criticality as described in the [COV Data Governance Policy]. A sample set of classifications is shown below.

| **Classification** | **Description** | **Security** |
| --- | --- | --- |
| **Public** | Data that can be freely shared without any restrictions. | No encryption |
| **Internal/General** | Data intended for internal use within the organization. Can be shared with business guests and external partners as needed. | No encryption |
| **Confidential** | Data that requires protection due to privacy, legal, or regulatory reasons. Used on sensitive business data which could cause hard is over-shared.  Additional Labeling (optional)  **Confidential – [Agency] Extended** (FTEs, contractors, trusted partners)  **Confidential – [Agency] Internal Only** (FTE’s only)  **Confidential – [Agency]/[Project Only**] (Agency/project specific label)  **Confidential – Recipients Only** (only selected recipients) | Protected using Rights Management, masking and encryption |
| **Restricted/Highly Confidential** | Highly sensitive data that requires stringent access controls and security measures.  Additional Labeling (optional)  **Highly Confidential – [Agency] Extended** (FTEs, contractors, trusted partners)  **Highly Confidential – [Agency] Internal Only** (FTE’s only)  **Highly Confidential – [Agency]/[Project Only**] (Agency/project specific label)  **Highly Confidential – Recipients Only** (only selected recipients) | Protected using Rights Management, masking and encryption |

## Compliance and Monitoring

* The Data Owner and Data Steward must conduct regular audits to ensure compliance with data stewardship policies.
* The Data Steward and the ISO must monitor data access and usage for unauthorized activities.
* The Data Steward and the ISO must report and respond to data breaches in accordance with incident response procedures.
* Compliance with this policy is mandatory for all departments and individuals involved in dataset management.
* Non-compliance may result in corrective actions as determined by the [Agency] leadership.

## Training and Support

* The Data Steward must provide training for all employees on data stewardship policies and best practices.
* The Data Steward must promote a culture of data responsibility and awareness throughout the organization.

## Policy Review

This Policy will be reviewed and updated annually from the approval date, or more frequently if appropriate. Any staff members who wish to make any comments about the Policy may forward their suggestions to [AGENCY Contact].

## Related Policies

|  |
| --- |
| **[AGENCY] Policies, Standards and Procedures** |
| Data Governance Policy |
| Data Quality Policy |
| Metadata Management Policy |
| Data Security Policy |
| Data Retention Policy |
| Data Privacy Policy |

The [Agency] adheres to all Commonwealth Information Technology Resource Management (ITRM) policies and standards for security and architecture [Policies, Standards & Guidelines | Virginia IT Agency](https://www.vita.virginia.gov/policy--governance/policies-standards--guidelines/).

|  |  |
| --- | --- |
|  | **VITA Related Policies** |
| IT Information Security Policy - SEC519 |
| Information Security Standard - SEC530 |
| IT Risk Management Standard - SEC520 |

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Revision Date** | **Description of Change** | **Author** |
| V1 | 6/10/2024 | Initial Draft | Chris Burroughs |
|  |  |  |  |
|  |  |  |  |