INFORMATION MANAGEMENT AND SECURITY STANDARD

Data Steward

Approved By:	**Information Management and Security Governance Committee**
Parent Policy:	**Information Management and Security Policy**
Effective Date:	**2022/05/31**
Next Revision Due:	**2026/05/31**
Business Unit:	**Collaboration, Analytics & Innovation, Information Technology**

GENERAL

This Standard is an extension of the Information Management and Security Policy. Consequences of non-compliance with this Standard are outlined in the Policy.

PURPOSE

This Standard outlines the responsibilities of Data Stewards for ensuring proper quality, security, privacy, confidentiality, lifecycle, and access to Data.

SCOPE

1.1. This Standard applies to Data Stewards.

1.2. This Standard applies to all City of Calgary Data.

1.3. This Standard does not apply to Data owned by external parties. These groups are responsible for governing the collection and use of their own Data.

DEFINITIONS

a. **"Data"** means any facts, concepts, quantities, characters, or instructions stored and/or transmitted in electronic formats;

b. **"Data Steward"** means a subject matter expert that defines, produces or uses Data as part of their role and has a defined level of responsibility for assuring quality in the definition, production or usage of that Data;

c. **"Dataset"** means a collection of related sets of Data; and,

d. **"Technology Steward"** means an individual who provides support and is associated with specific systems, applications, Data stores, and technical processes.

STANDARD DETAILS - CLAUSES AND SUBCLAUSES

RESPONSIBILITIES

Directors are responsible for ensuring Data Steward responsibilities are assigned to a role and maintained over time.

Data Stewards are responsible for the following:

- Applying the Information Management & Security Policy and associated standards and guidelines to which they must adhere;
- Informing Data users regarding the metadata and business rules affecting the Data to ensure awareness of its proper usage;
- Engaging stakeholders and Data users regarding any changes, issues, security, and general usage of Data;
- Maintaining, identifying, and registering metadata under the Dataset;
- Being the primary contact for any Data related inquiries;
- Determining and providing appropriate Information Security Classifications for the Data;
- Sharing Data in accordance with the *Access and Sharing Standard* and *Open Data Standard*;
- Reviewing for Data usage, users, access levels, and for Data quality;
- Staying informed of changes to corporate policies affecting Data privacy, standards, guidelines, and lifecycle; and,
- Ensuring business continuity for their respective Data Steward role.

Technology Stewards are responsible for:

- Identifying changes to the Data that may affect other systems, processes, databases, Data formats, or metadata, and informing impacted groups;
- Consulting when new Data is created, or changes are made to the Data, including Data structure, Data flows, Data quality/integrity criteria, Data integrations and testing;
- Consulting for initiatives/projects creating new Data or affecting existing Data such as new uses, integrations, and where Data is used for a different purpose or takes on a different role;
- Guiding business units regarding the collection, processing, and storage of City Data; and,
- Assisting Data Stewards with appropriate tools and the profiling of Data in applications.

ACCOUNTABILITIES

Directors are accountable for providing executive support and endorsement for Data Stewards.

Data Stewards are accountable for:

- Ensuring Data quality and integrity criteria are defined and applied to the Data;
- Ensuring the metadata and business rules applicable to the Data are captured and maintained;
- Working with Access & Privacy, Corporate Security, and Information Technology to ensure necessary audits and reviews are in place at a proper frequency and that conflicts, questions, challenges, and Data quality issues are addressed;
- Completing Privacy Impact Assessments (“PIA”) and updating the PIA when changes are made to the Data;
- Verifying rules for Data retention, repatriation, and destruction are appropriately applied following the requirements of Data lifecycle and the Corporate Records Management Program;
- Confirming all Data and related materials are stored within an accessible repository; and,
- Ensuring that the end user understands rules concerning Data quality and how metadata is defined.

RESOURCES

Refer to the Administration Policy Library for the following:

- Information Management and Security Policy
    - Access & Sharing Standard
    - Electronic Communications Standard
    - Information Security Classification Standard
    - Intellectual Property Standard
    - Open Data Standard
- Protection of Privacy Policy
- Records Management Policy, Standards and Guidelines

REVISION HISTORY

Review Date	Description
2022-05-31	New standard approved by the Information Management Security Governance Committee
2022-06-07	Edits made at the request of the Information Management Security Governance Committee