INFORMATION MANAGEMENT AND SECURITY

Access and Sharing Standard

Approved By: Information Management Security Governance Committee
Effective Date: 2022/04/26
Next Revision Due: 2025/04/26
Department / BU: Collaboration, Analytics & Innovation

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

The Information Management and Security Policy states, “City of Calgary Information that meets requirements outlined in the associated Information Management and Security Standards will be made available to Authorized Users, including the public, either proactively or upon request.”

This Standard outlines the requirements for access and sharing of internal and external Information Assets with Authorized Users.

SCOPE

This Standard applies to all Information Assets that are within the scope of the Information Management and Security Policy.

DEFINITIONS

"Authorized User" means an individual who has been granted access to use City Information Assets or Information Systems; Authorized Users may be internal users (City employees) or External Users;

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

"External Users" means the public, citizens, contractors, consultants or service providers working on behalf of The City; members of Council and Council staff; the Mayor and staff of the Office of the Mayor; boards, commissions and committees appointed by Council; Calgary Police Service; civic partners; other governmental organizations and approved researchers.

"Information" means any collection of Data that is processed, analyzed, interpreted, classified, or communicated to serve a useful purpose, present facts, or represent knowledge;

"Information Asset" means Information recognized as having value for the purpose of enabling The City to perform its business functions, thereby satisfying a recognized business requirement. There are many types of Information Assets. Information Assets can include Data and Intellectual Property;

"Information Steward" means any Authorized User responsible for the management of specific Information Assets or Information Systems;

"Intellectual Property" means all trademarks, marks, copyright, art, inventions, creative works, reports, Data, compilations of Information, computer programs, drawings, sketches, layouts, commercial material, working papers, documents, copy, ideas, photographs and negatives, films, videotapes, video, audio and audio-visual productions and other materials in all forms and however fixed, stored, expressed or embodied, created, developed, generated, authored or produced.

"Open Data" means the practice requiring that certain Data be made freely available to the public, in machine readable format without restrictions from copyright, patents or other mechanisms of control.

"Personal Information" means the Recorded Information about an identifiable individual as defined in Section 1(n) of the Alberta *Freedom of Information and Protection of Privacy ("FOIP") Act.*

STANDARD DETAILS - CLAUSES AND SUBCLAUSES

1. INFORMATION ASSET CLASSIFICATION

The labelling of Information Assets as Unrestricted, Confidential, or Restricted must meet the classification criteria set out in the Information Security Classification Standard.

2. ACCESS AND SHARING WITHIN THE CITY

Information Assets should be shared internally wherever possible and appropriate to further business activity and facilitate knowledge reuse.

a. Requesting Access

All internal requests for access to Information will be directed to the appropriate Information Steward, who shall grant access to or share the Information.

If an Authorized User has been denied access to Information and that denial cannot be reasonably resolved, then the requestor may bring forward a request to the Information Management and Security Governance Committee for resolution.

b. Personal Information

Authorized Users with access to Personal Information must ensure that this Information is properly safeguarded. A Privacy Impact Assessment (PIA) or Access Impact Assessment (AIA) or both must be completed before access to Personal Information is granted or Personal Information is shared. All security and privacy recommendations made as part of those assessments must be implemented and adhered to.

Personal Information can only be used for the purposes for which it was originally collected. A documented business need is required to provide access to Personal Information. All Personal Information (electronic or paper) must be clearly identified as such.

c. Transmission Mechanisms

Information handling procedures as outlined in the Information Security Classification Standard must be followed. Wherever possible, access should be granted by the Information Steward to the original source file with proper security and access controls in place to prevent duplication of Information or insecure transmission.

The Information Steward can define the type of access (e.g. read-only or write access) to electronically stored Information. If copies are provided (either electronically or in physical form), the Authorized User is expected to secure those copies to the same level as the original Information Asset, as defined in the Information Security Classification Standard. Copies must also be managed to the same lifecycle requirements as the source file.

3. ACCESS AND SHARING OUTSIDE OF THE CITY

Information Assets created and maintained by The City are often shared externally. Sharing of Information Assets for the benefit of citizens and the whole of The City of Calgary is encouraged, but Authorized Users must follow proper procedures to manage risk.

a. Access and Sharing of Unrestricted Information Assets

Routine disclosure of "Unrestricted" Information is highly encouraged. Routine disclosure involves sharing through existing and approved means, such as Calgary.ca, City Archives, or the Open Data Portal.

Information Stewards should publish Unrestricted Data on the Open Data Portal whenever possible.

b. Access and Sharing of Confidential Information Assets

All external access to, or sharing of, Information Assets is managed by Collaboration, Analytics & Innovation (CAI). External access requests will be directed to both CAI and the appropriate Information Steward. If the external request does not fall under a pre-existing legal agreement, then CAI will create a license agreement for that request.

All legal agreements and related procedures with respect to external sharing of Information are managed by CAI. Records of legal agreements for external use are maintained by CAI in accordance with corporate records management practices.

Access Mechanisms for Confidential Information Assets:

Proposed Use	Access Mechanism
Approved Vendors, Contractors, and Consultants	• If successful in a bid, the Supply Management Terms and Conditions address data sharing • Otherwise, executed license agreement
Any other use including commercial	• City Online • Executed license agreement

Information Stewards should contact CAI about publishing Confidential Data on City Online.

i. Security

Sharing of Information externally carries unique security risks. If CAI identifies that a PIA or AIA is required, access will be provided only after all concerns related to the assessment(s) have been satisfied.

ii. Personal Information

Personal Information must never be exchanged externally, including with municipal partners, without prior authorization of the Access and Privacy Section and completion of a PIA. Personal Information can only be used for the purposes for which it was originally collected.

c. Access and Sharing of Restricted Information Assets

External access is NOT provided to Information Assets classified as Restricted.

d. Fees

Fees, including royalty payments, may be applied to external access requests; however whenever possible, Information Assets will be provided at no cost. CAI has the authority to grant a fee waiver if it is deemed to be in The City's best interest to supply the Information at no cost.

If fees are attached to Unrestricted Information Assets, they will not exceed the preparation and distribution cost.

Fees may be applied to requests for Confidential Information Assets. The Information Steward, along with CAI, will determine the market value of the Information Asset. If the market value is less than the potential societal benefits, The City will provide the Information Asset to requestors at no charge. A legal agreement will still be required.

Where appropriate, distribution of Information Assets may require royalty or payment schedules to The City. Distribution of revenues from licensing is the responsibility of the City Treasurer.

e. Access to Information Requests

All requests for Information made through a Freedom of Information and Protection of Privacy Act request are done so under the provisions granted therein and may supersede those outlined in the Information Management and Security Policy and its associated Standards.

4. ACCESS AND SHARING COMING INTO THE CITY

a. Licensing External Data

Structured datasets purchased from third parties should be provided under a license agreement. City of Calgary staff should contact CAI to assist with developing terms for an agreement. Whenever possible, terms should state agreement is made with "The City of Calgary" to ensure that data is made available to all City employees.

RESOURCES

Refer to the Administration Policy Library for the following:

- Information Management and Security Policy
  - Information Security Classification Standard
  - Open Data Standard
- Protection of Privacy Policy
- Corporate Records Management Policies and Program

REVISION HISTORY

Review Date	Description
2018/01/30	New Access and Sharing Standard reviewed and approved by Information Management and Security Governance Committee. (Replaces External Data Access and Management Policy)
2022/04/26	Amendment approved by Information Management and Security Governance Committee