Analysis of The City's Current Privacy Practices

Contents

Collection of Personal Information Process and Intended Use

One of the purposes of the Freedom of Information and Protection of Privacy Act ("FOIP Act") is "to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information". Public bodies cannot collect personal information unless the collection is authorized under the FOIP Act.

FOIP Act

Collection of Personal Information

No personal information may be collected by or for a public body unless:

a. The collection of that information is expressly authorized by an enactment of Alberta or Canada,
b. that information is collected for the purpose of law enforcement, or
c. that information relates directly to and is necessary for an operating program or activity of the public body.

Manner of Collection of Personal Information

The FOIP Act provides that, subject to some limited exceptions, a public body must collect personal information directly from the individual.

THE CITY OF CALGARY
EXCEEDS LEGISLATED REQUIREMENT

Current Privacy Practices

Privacy Impact Assessments ("PIAs")

PIAs are not mandatory under the FOIP Act. In 2007, The City of Calgary (The City) adopted an Administration Policy on *Privacy Impact Assessments (PIA)* (GN-022) requiring that all City projects, practices and information technology systems that involve the collection, use or disclosure of personal information undergo a PIA.

WHAT
Identifies privacy risks of a project , information technology or program. Identifies privacy risks with third party services or technology providers.

WHEN
At the start of a new project or development of information technology, or when a change to an existing project that uses or discloses personal information.

RECOMMENDS
Ways to reduce privacy risks through controls, administrative, technical or physical safeguards, data minimization or other mitigation.

WHY
Ensures protection of citizen data. Ensure compliance with legislated requirements for the reasonable security and protection of personal information.

Requests for PIAs are submitted to City Clerk's Access and Privacy for evaluation. During the preliminary review phase, projects are assessed to determine if the information collected would be considered personal information, the authority for collection, the intended use and the context under which it will be shared internally or externally and how it will be safeguarded.

The PIA process connects with key stakeholders in Corporate Security, Information Technology and business units to understand privacy, security or technical risks associated with collection, use and/or disclosure of personal information and develop mitigation controls.

2018	PIA RECEIVED BY ACCESS AND PRIVACY	65
	PIA COMPLETED BY ACCESS AND PRIVACY	60
2019	PIA RECEIVED BY ACCESS AND PRIVACY	109
	PIA COMPLETED BY ACCESS AND PRIVACY	59

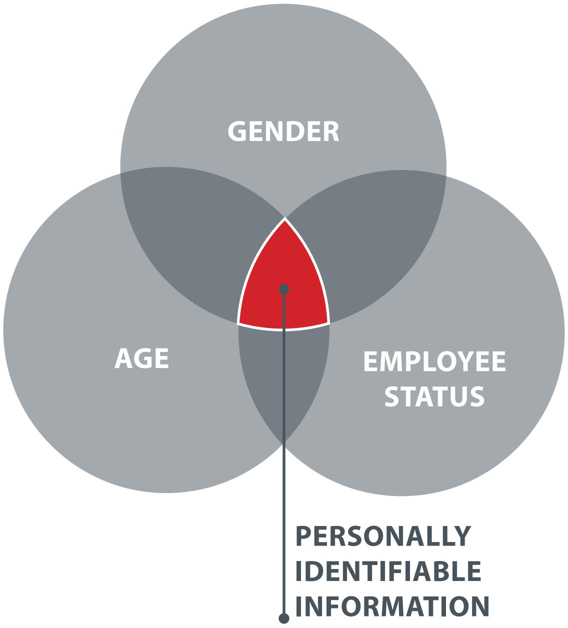
PIAs are living documents revisited as technology or systems change.

PIA Process

- CORPORATE PIA INTAKE AND REVIEW (ACCESS & PRIVACY)
- CLIENT AND STAKEHOLDER MEETING
- IDENTIFY PRIVACY RISKS OF PROJECT (ACCESS & PRIVACY)
- PRIVACY ANALYSIS (ACCESS & PRIVACY)
- PRIVACY RECOMMENDATIONS (ACCESS & PRIVACY)
- CLIENT AND STAKEHOLDER MEETING
- PIA REPORT (ACCESS & PRIVACY)

Future State

Anonymization, de-identification and pseudonymization
Emphasize removing personal identifiers, separation and altering of data to break linkages to an individual's identity, remove risks and eliminating the possibility of creating a mosaic effect.



A mosaic effect is when disparate information sources are combined to identify an individual.

Data Mapping
Emphasize flow of data, not just the flow of personal information, through lifecycle to prevent commingling and linkages to an individual's identity.

Context
Emphasize the context in which personal information and/or data will be disclosed and the possible consequences of intended further use.

PIA Auditing
Formalize annual reviews and assessments of completed PIAs to ensure that the collection scope, intended use and technology have not changed. Increasing audit abilities will help ensure personal information is protected even as technology and processes evolve.

Tracking, Mitigation and Remediation Activities
Create a central repository and implement new technology to track and follow up on privacy recommendations on an ongoing proactive basis.

Interconnected Devices
Emphasize privacy in the development and design of interconnected processes, programs and devices.

Privacy Awareness in Data Analytics
Ensure privacy is not compromised and individuals will not be re-identified during data analysis and publication in open portals.

Updated PIA Policy
Proactive, not reactive, policy that is aligned with privacy practices of the European Union's General Data Protection Regulations to prepare for Smart Cities.

Threat Risk Assessment ("TRA")

A comprehensive information security risk assessment is completed collaboratively with stakeholders in City Clerk's, Corporate Security, Information Technology and various business units. The goal of the risk assessment is to assess information security risks, including identifying personal information collected or contained in new information systems or applications, and provides guidance on risk mitigation strategies to reduce risk.

2018 TRA COMPLETED BY CORPORATE SECURITY 41

2019 TRA COMPLETED BY CORPORATE SECURITY 64

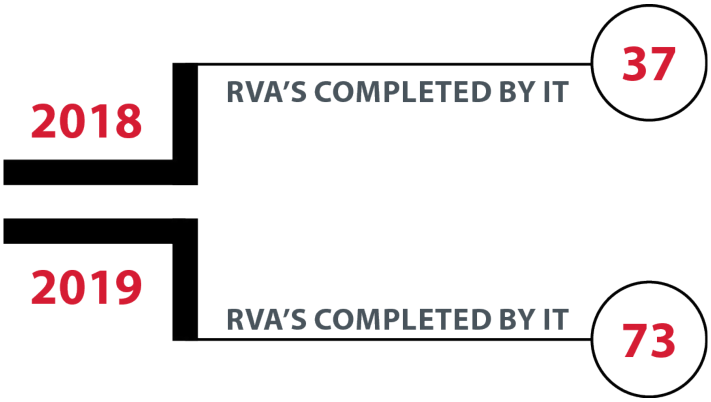
Future State

Tracking
Implement new technology that allows tracking and managing application and data risk. Having a central repository of TRA's will show trends in risk and better manage and track data risk.

Cloud Risk Value Assessments ("RVA")

Information Technology's Cloud Computing and Open Source Program helps business units evaluate and adopt solutions to meet their business needs. TThe program works with the business units, other Information Technology divisions, Law, City Clerk's Office, Corporate Security and Information Management, as well as industry experts, suppliers/vendors. The program team facilitates a Risk Value Assessment ("RVA") which focuses on data protection, data security & ownership and privacy. The RVA helps the business make an informed decision on whether the cloud solution requested is a viable business and technology option.

Through the Cloud RVA, an in-depth evaluation is completed of access management, vendor's third-party service providers, vendor's incident and security breach policies, and current security standards and certifications.



2018 RVA'S COMPLETED BY IT 37

2019 RVA'S COMPLETED BY IT 73

Future State

Increased Risk Management and Alignment
The Cloud and Open Source Program is moving from current risk identification to risk life cycle management - through awareness & engagement across information management stakeholders and City staff. The Cloud RVA process should be integrated with The City's Risk Register to ensure all high impact and high probability items captured in the Cloud RVA's are properly tracked. Risks identified with high probability and high impact will be assigned and mitigated with recommendations to the business using the service. The recommended mitigations will be tracked and validated to ensure that they are being effectively managed.

Current risk identification processes will be enhanced to include concepts of risk appetite, and risk tolerance with technology and business stakeholders. Stakeholder engagement will discuss the current risk landscape, current and future business initiatives that may lead to excessive risk and how to assess risk prioritization and risk mitigations.

FOIP Act

Notification of Collection of Personal Information

A public body that collects personal information must inform the individual of:

a. The purpose for which the information is collected,

b. the specific legal authority for the collection, and

c. the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

THE CITY OF CALGARY
MEETS LEGISLATED REQUIREMENT

Current Privacy Practices

Notification of Collection of Personal Information

Notification allows individuals to know the authority for the collection of personal information, the purpose for collection and how the personal information will be used. Notification also identifies who can be contacted at The City to explain why the personal information is being collected, how it will be used and/or disclosed. Notification of collection of personal information is given in several ways at The City:

FORMS AND APPLICATIONS

- Hard copy
- Online

PUBLIC SPACES

- Posters
- Displays on service counters

VERBALLY

- In person
- Phone pre-recordings

Future State

Public Awareness
Emphasize public notification and awareness, provided in a manageable and easily accessible manner. Use best tools to reach Calgarians to bring awareness to The City's privacy program, including access to information and the ability to request a correction of personal information in The City's custody or control.

FOIP Act

Use of Personal Information

A public body may use personal information only

a. for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
b. if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
c. for a purpose for which the information may be disclosed to that public body under sections 40, 42 or 43 of the FOIP Act.

A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

THE CITY OF CALGARY
MEETS LEGISLATED REQUIREMENT

Current Privacy Practices

Use of Personal Information

The City engages many processes and procedures to guard against improper use of personal information in its custody or under its control:

+ The PIA process enables data use minimization by ensuring the collection of personal information is limited and the use is consistent with the purpose of collection. Once a PIA is submitted to Access and Privacy, personal information flows are examined to ensure compliance with the FOIP Act. In some instances, the flow of personal information may need to be altered due to a use of personal information that is inconsistent with the collection or not required.
+ The City has policies in place to control the use of personal information. These policies define the classification of information and clearly define how technology can be used to store, transmit and use information of different classifications.
+ The City employs technical controls and auditing to limit data exposure and restrict access to those that have a business need. These controls include access control, email management systems, file auditing and security and application level security.
+ The City provides various training courses to employees on the use and disclosure of personal information.

Future State

Anonymization, de-identification and pseudonymization
Emphasize removing personal identifiers, separation and altering of data to break linkages to an individual's identity, removing risk and eliminating the possibility of creating a mosaic effect.

Personal Information Handling Practices

The City collects personal information necessary for City Departments to provide service to the public, and to coordinate the delivery of services. The City uses personal information only to the extent necessary to carry out its purpose in a reasonable manner. While in The City's custody, Information Technology and Corporate Security take steps to safeguard the integrity and security of personal information. Depending on the type of personal information, The City may implement administrative, physical and/or technical safeguards to secure the personal information during its lifecycle.

FOIP Act

The FOIP Act provides that the head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

THE CITY OF CALGARY
EXCEEDS LEGISLATED REQUIREMENT

Current Privacy Practices

Administrative Safeguards

City employees and third parties have access to administrative policies and training to bring awareness to their responsibilities related to information management, security and privacy.

Administrative Policies

The City's Administration policies identify roles and responsibilities for positions related to the management of privacy (FOIP Head/ City Clerk), security (Chief Security Officer) and information technology (Chief Information Technology Officer) within The City. The Administration policies also provide clear direction to staff on the appropriate handling and protection of personal information. TThese Administration policies, and associated Standards and technical controls, are available to staff in The City's Administration Policy Library.

Training

Training programs are available to City employees (online and in person) to bring awareness to responsibilities related to privacy and security. For example:

- **All City employees:**
  - Mandatory Code of Conduct training, which includes modules on the FOIP Act and Acceptable Use of City Technology Resources;
  - Optional Access, Privacy, and Information Management Security courses (online and in person)
- **New hires:**
  - Required to take City of Calgary Orientation ("COCO"), which includes modules related to access and privacy.

With respect to third parties, The City enters into written agreements when an outside agency or contractor is collecting personal information on behalf of The City.

In person access and privacy training is available to third parties conducting business on behalf of The City.

Physical Safeguards

Access and authorization mechanism (employee access cards) are in place to restrict access to authorized individuals. Physical Security Risk assessments are completed on priority sites and physical security systems are in place to protect sites and information assets.

Secure filing rooms and cabinets can be provided for personal information storage which include access control mechanisms.

Technological Safeguards

In collaboration with Corporate Security, City Clerk's, Corporate Analytics and Innovation, Information Technology manages all information assets in The City's possession by controlling and restricting access to and protecting The City's technical infrastructure (hardware and software). With the extensive use of third-party technologies, services and tools, Information Technology provides:

- Access controls on devices
- Access control for applications and databases
- Risk management
- Intrusion protection
- Usage restrictions
- Virus protection
- Network security

This ensures the right people are accessing the right information they need to perform their jobs. Information Technology makes use of these technologies to monitor, audit and report on all aspects of our technical environment to ensure compliance to each of the pertinent policies. Information Technology, Corporate Security and City Clerk's Office provides education on usage and standards to help ensure staff are using technology correctly.

Future State

Mandatory Access and Privacy Training for City Staff

Making privacy and information handling training mandatory will ensure all staff and contractors are aware of proper handling of personal information and their role in the protection of personal information.

Privacy Awareness for the public

Communicate The City's safeguarding practices to protect against such risks as unauthorized access, collection, use, disclosure or destruction.

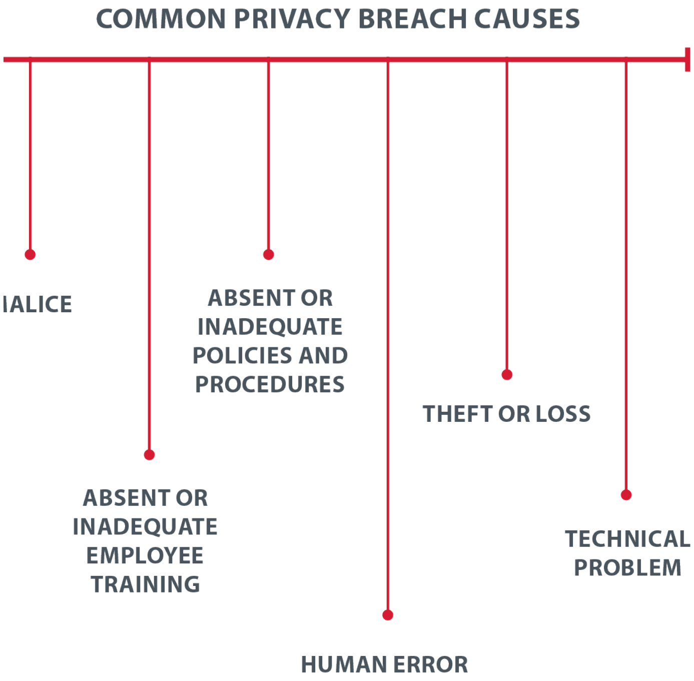
Privacy Settings

Periodic review of information technology infrastructure, identifying ways to improve service delivery, protect data and remain secure in an evolving technical landscape. This process has and will continue to emphasize protection of personal and sensitive data.

Anonymization, de-identification and pseudonymization

Emphasize removing personal identifiers, separation and altering of data to break linkages to an individual's identity and remove risk of creating a mosaic effect.

Privacy Breach Management and Notification


COMMON PRIVACY BREACH CAUSES
IALICE
ABSENT OR INADEQUATE POLICIES AND PROCEDURES
THEFT OR LOSS
ABSENT OR INADEQUATE EMPLOYEE TRAINING
TECHNICAL PROBLEM
HUMAN ERROR

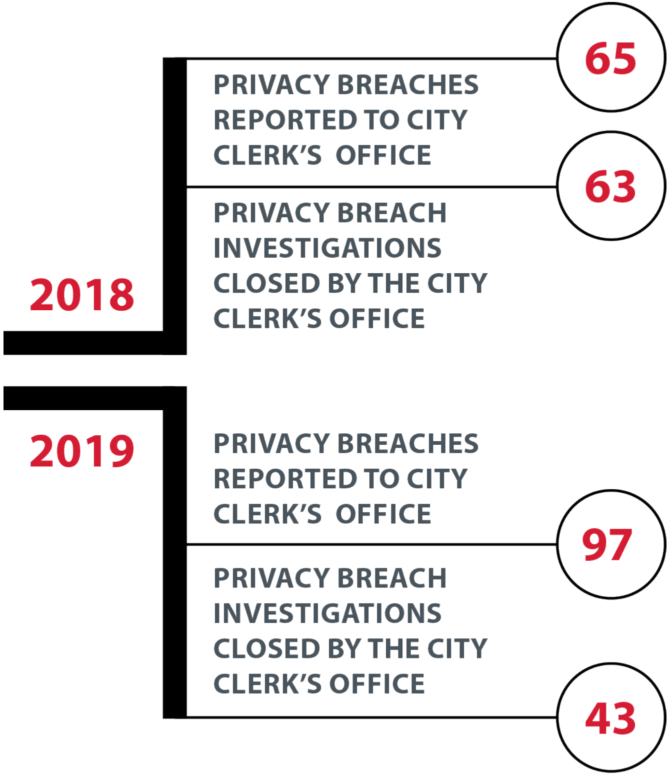
Responsibilities for privacy incident and breach management are defined at The City. The FOIP Head has the overall responsibility for the protection of privacy, and works collaboratively with Corporate Security and Information Technology, as required. The Chief Security Officer is responsible for incidents and breach management that does not involve personal information.

Although not required by law, The City notifies affected individuals and the Office of the Information Privacy Commissioner of Alberta (OPIC) following a comprehensive assessment of a real risk of significant harm to an individual as a result of personal information loss, unauthorized access or disclosure.

The City's approach to notification models the Personal Information Protection Act ("PIPA") provision, which states that it is mandatory for an organization with personal information under its control to notify the Information and Privacy Commissioner without delay, of a privacy breach where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

Effective 2018, Access and Privacy:

- Investigates every privacy breach report, internal and external, and provides a Letter of Findings to the business unit's senior management, including recommendations regarding future risk avoidance.
- Conducts annual reviews of privacy breaches to identify patterns and develop prevention strategies.
- Delivers regular in person and online privacy awareness training sessions to City employees handling personal information and those who were involved in a privacy incident or breach.
- Audits compliance and implementation of recommended administrative, physical or technical safeguards against further privacy breaches.



Future State

Privacy Protocol

Formally document the privacy incident and breach management program and its protocols, including notification of affected individuals and the OPIC. This process has and will continue to emphasize protection of personal and sensitive data.

Determination of Severity and Harm

Document the current process to identify severity and risk of harm to affected individuals.

Privacy Breach Notification

Evaluate current and implement improvements to the notification standards.

FOIP Act

An employee, in relation to the public body, includes a person who performs a service for the public body as an appointee volunteer or student or under a contract or agency relationship with the public body.

THE CITY OF CALGARY
MEETS LEGISLATED REQUIREMENT

Current Privacy Practices

Third Party Protection of Personal Information

The City engages third-party service provider to supply a service which is managed by The City. In these instances, the third-party service provider is an 'employee' of The City, as such, has a duty under the FOIP Act to protect the personal information that it collects, uses and discloses as part of that service. Online and in person privacy awareness training is available to third party providers.

By engaging the PIA process when selecting service providers, The City can ensure service providers limit collection of personal information, have adequate safeguards in place to protect personal information it collects, uses and discloses, and will dispose of the personal information after the purpose of the collection has been completed.

Information Technology's Cloud Computing and Open Source Program helps business units evaluate third party providers.

Future State

Compliance
Implement follow up on compliance with contractual obligations, e.g. third party confirmation that personal information has been securely destroyed.

Personal Information Retention Policies and How Consistently They Are Observed

The classification and retention policies for The City are set out in City of Calgary Bylaw 53M99, being a bylaw to adopt policies and procedures for the management of The City of Calgary's records including classification and retention schedule pursuant to the Municipal Government Act 1994 S.A. M-26.1 ("Bylaw 53M99").

FOIP Act

The FOIP Act provides that if an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must retain the personal information for at least one year after using it to make a decision, so that the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by:

a. The individual,
b. The public body,
c. If the body that approves the records and retention and disposition schedule for the public body is different from the public body, that body.

Bylaw 53M99

Bylaw 53M99 sets out that The City will retain Corporate records until they have met operational, legal and fiscal purpose and that when records have met their retention requirements the disposition process will be implemented.

THE CITY OF CALGARY
MEETS LEGISLATED REQUIREMENT

Current Privacy Practices

Personal Information Retention Policies

Bylaw 53M99 is supported by a robust Corporate Records Management Program which ensures that business units are provided with support, guidance and processes on how to effectively identify and manage Corporate records. Administration policy on *Records Disposition* (GN-013(B)), provides that Corporate Records are retained until they have met operational, legal and fiscal purpose, at which time they are disposed of by destruction, deletion or transfer to the Archives.

Annually, the City Clerk's Office provides each business unit with a listing of records that have met retention periods as set out in the Corporate Records Classification and Retention Schedule and are ready for disposition.

Disposition of records, which may contain personal information, may be delayed or suspended because of an audit, a legal action, a change in legislation, a FOIP request, or a change in the use of a record or record series.

In 2016, the disposition of records that had met their retention was suspended as City Clerk's, in conjunction with Information Technology, upgraded and modernized The City's records management system. Disposition of records that have met retention requirements resume in Q4 of 2019.

Future State

Electronic Disposition Process
Implement a digital disposition process for electronic records that adheres to the Corporate Records Bylaw and policies.

Awareness Training
Implement online training on records management, retention and disposition practices.

Use of Third-Party Services or Technologies

The City maintains a complex and robust network of technologies and services that enable The City to meet Citizen's needs in an efficient and effective way. Information Technology is a corporate service responsible for the management and support of The City's technical infrastructure, and the development/acquisition and support of the software installed on it. This includes servers, databases, computers and mobile devices, all of which pass information across The City's network and wireless infrastructure. In collaboration with Corporate Security, City Clerk's, Corporate Analytics and Innovation, Information Technology manages all information assets in The City's possession by controlling and restricting access to and protecting our technical infrastructure (hardware and software). Information Technology develops and maintains both corporate-wide and line-of-business applications and improves and automates business processes to enable City business units to deliver internal and citizen-facing services, while respecting personal information.

FOIP Act

The FOIP Act provides that "the head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use disclosure or destruction".

THE CITY OF CALGARY
MEETS LEGISLATED REQUIREMENT

Current Privacy Practices

Data Protection of Personal Information

Information security design is part of all systems and infrastructure architecture design; Information Technology technical processes, business practices and methodologies follow City policies and standards; and plans for business continuity are in place.

All data located on City websites and in email, software applications, databases, files (documents, spreadsheets, images, etc.) and other information repositories supported by Information Technology are managed, protected and monitored. Third party technologies provide:

- Email protection from spam and malware;
- Secure processing of financial transactions;
- Reporting and alerts;
- Various means of restricting changes to our systems;
- Secure web traffic transmission and protection of files, among others.

User Authentication

Systems and procedures are in place to authenticate users. The City requires user name and password, two-factor authentication (for remote access), certificate, external token, or biometrics before access is granted to systems handling personal information.

Unstructured Data Security Initiative

Information Security is currently leading a security audit and remediation of all access controls and file system permissions. The goal is to identify and validate the security controls in place for sensitive information. The project is currently in pilot with five (5) Business Units slated to be complete in 2019. The objectives of this project are to review existing access, classification of information and identify any personal information and where appropriate recommend strategies to reduce risks and modify access controls.

This project is the foundation for role-based access where individual data owners will control (approve and revoke) access to information based on who has a business need to access that information.

Device Management

Information Technology uses tools to manage The City's desktop, laptop and thin-client computers which provide standardization for how they are built and installed, hard drive encryption, enforcement of security rules, regularly updated security patches, and the ability to lock them down remotely in case of theft and remote administration and monitoring.

To help ensure business continuity and protection of data, Information Technology keeps The City's third-party technologies and services up to date and stable to ensure the latest security protections are in place. This includes operating systems, servers, databases, computers and mobile devices, as well as The City's wired and wireless networks.

City administrative policies restrict the use of unapproved hardware and software for storing personal information. This includes personal devices, removable media (thumb drives) and hosted software without appropriate identity management and authentication.

Logging and Monitoring

User access to personal information (e.g. viewing, modification, deletion of records) both from a front-end (e.g. business user) perspective and a back-end (e.g. system or database administrator) perspective is logged and monitored on a regular basis in accordance with the Access Control Standard (Information Management and Security Policy). Efforts are underway to ensure all locations and systems which contain personal information generate logs which are directed to a security and event monitoring process to identify unauthorized access or suspicious user activity. These events are monitored and reviewed by the Corporate Security Information Security Operations Team.

As part of the Unstructured Data Security Initiative files and folders containing personal information are being identified and Corporate Security (Information Security), supported by City Clerk's Office offer remediation options to ensure proper security and alerting are in place for these highly sensitive files.

Change Control

Information Technology maintains a change control process which ensures that new implementation and modifications to systems follow strict change control processes to ensure system data is not exposed.

Open Data Practices

Open Data supports The City's position as an open organization by increasing transparency, improving public participation and enhancing services for citizens.

The City of Calgary Digital Strategy embeds the concept of "open by default" in the section "We are transparent":

- Data belongs to citizens. If The City collects data it will go in the Public Catalogue.
- Only closed to protect privacy and to provide security. Information will be shared in a manner such that it will not impact the privacy of individuals. Privacy and security are not an afterthought; they are part of the design.

The City's Open Data Strategy aligns with the International Open Data Charter in coupling the principle of "Open by default" with the recognition that open data must not compromise citizens' right to privacy.

External access to data and information

In alignment with the International Open Data Charter, Principle 1, Section 4: "We recognize that open data can only be unlocked when citizens are confident that open data will not compromise their right to privacy, and that citizens have the right to influence the collection and use of their own personal data or of data generated as a result of their interactions with governments."

The City's ability to release Open Data to the public is strengthened by the policies and processes surrounding the collection, storage and management of that information earlier in the data lifecycle.

THE CITY OF CALGARY IN PROCESS OF

ALIGNING TO INTERNATIONAL STANDARDS

Current Privacy Practices

Practices to prevent external release of personally identifying information

External access to City data is centrally managed within Corporate Analytics and Innovation, including:

- Open Data
- Data licensing and Information Sharing Agreements
- Sharing data with City vendors and contractors

This centralization is intended to ensure all external data access adheres to policy, and there are work-flows to guard against the release of personally identifying information. When there is a request for external access to City data, this team works to identify the appropriate data steward and understand the data required to fulfill the request. Analyzing the data's suitability for external access relies on:

- Information Security Classification
- Relevant Privacy Impact Assessments for the collection, use and disclosure of personal information
- The structure and content of the data

Most datasets provided externally come from sources that do not contain personal information (e.g. information about City assets). For data that contains potentially personally identifying information, appropriate mitigation strategies are developed, or data release is not recommended. Some of the mitigation strategies used to decrease the risk of personal identification include:

Anonymizing (removing) or pseudonymizing (replacing) fields containing personally identifying information. E.g. removing the owner’s name from a dataset of property information.

Generalizing or aggregating data to reduce the risk of re-identifying an individual. E.g. aggregating Civic Census data to the community or ward level.

Partial release – not releasing data fields containing personal information, or suppressing aggregate records that apply to very few (<10) individuals .

These strategies help ensure data provided externally does not contain direct personal identifiers (e.g. name, phone number, identifying numbers, etc.), but can contain indirect personal identifiers (e.g. age, gender, etc.) if proper precautions are taken to mitigate the risk of individuals in the dataset being re-identified.

If the required mitigation strategies are implemented, the data may be suitable for release externally, either licensed to specific parties, or as open data. The City’s Open Data Terms of Use provide an Open Government License for anyone to access and use the data for any purpose, including commercial uses, but includes exemptions that do not grant any right to use personal information.

Releasing personally identifying information for City business purposes

Approved external access to personally identifying information is rare, but sometimes required to deliver City services. When personally identifying information must be shared externally:

- The information must only be used for the purpose for which it was collected.
- The data is transferred using encrypted secure data transfer protocols.
- Parties sign a binding legal agreement including restrictions on use, distribution, retention and disposition.

Future State

Early de-identification

Support efforts to de-identify data as early as possible in the data lifecycle.

Open By Design

“Open by default” addresses the question of whether data is made available externally. “Open by design” addresses the processes and systems to safely and efficiently release open data, including planning for open data at the time of planning to collect data.