City Manager's Office Report to
Strategic Meeting of Council
2020 January 27

ISC: UNRESTRICTED
C2020-0039

City of Calgary Citizen Privacy Data Practices

EXECUTIVE SUMMARY

This report, in response to the Notice of Motion regarding *City of Calgary Citizen Privacy Data Practices*, provides an analysis of The City of Calgary's ("The City") current privacy practices, and brings forward a workplan for a strategic Privacy Framework to continue to uphold public trust in The City.

ADMINISTRATION RECOMMENDATIONS:

That Council:

1. Approve the Privacy Framework 2019-2021 Workplan (Attachment 1); and

2. Direct the City Clerk/FOIP Head to provide an annual report to the Priorities and Finance Committee on The City's Privacy Management Program.

PREVIOUS COUNCIL DIRECTION / POLICY

At the 2019 April 29 Combined Meeting of Council, Council adopted Councillor Diane Colley-Urquhart's Notice of Motion (C2019-0590), *City of Calgary Citizen Privacy Data Practices,* directing the Chief Security Officer/Chief Information Security Officer, the Chief Information Technology Officer, Chief Human Resource Officer and the City Clerk in consultation with appropriate City staff and leading external privacy experts to (a) provide an analysis of The City's current privacy practices; and (b) develop a visible, accessible and overarching strategic Privacy Framework associated with digital infrastructure ('Smart Cities') and a Workplan for implementation for Council consideration. Council directed Administration to report back directly to the January 27th, 2020 Strategic Meeting of Council, with a status update.

BACKGROUND

In Alberta, the *Freedom of Information and Protection of Privacy Act* ("*FOIP Act*") requires The City to protect the privacy of individuals by controlling the manner in which The City collects, uses and discloses personal information. While the *FOIP Act* sets out access and privacy requirements, and compliance with the *FOIP Act* is an obligation, it is the starting point for privacy practices at The City. The City also adopted bylaws, policies and procedures related to privacy (Attachment 2) to ensure that privacy is built into all City initiatives, programs, technologies and services. The City also delivers access and privacy awareness training to City employees and contractors related to their responsibilities (Attachment 3).

Municipalities, similar to other industries, are looking at ways to leverage data to enable efficiencies in program and service delivery. The City has been at the forefront of Smart Cities technology for several years. Initially, investing in critical connectivity, but more recently, developing the infrastructure to do Internet of Things ("IoT")/sensing required for a Smart City. Examples of Smart City initiatives are provided in Attachment 4. With Smart Cities comes a need for data governance in terms of policies, standards and procedures to ensure the protection of data. In 2019 September, The City was invited to be part of a Future Cities Canada initiative to develop and leverage data governance to support a Smart City initiative. A project team, comprised of subject matter experts from Information Technology, Corporate Analytics and Innovation, Corporate Security and the City Clerk's Office, has been established and tasked

with building a data governance framework that enables innovation while ensuring the protection of personal information.

INVESTIGATION: ALTERNATIVES AND ANALYSIS

In response to part (a) of the Notice of Motion, Attachment 5 provides an analysis of The City's current privacy practices. It indicates whether the current practices meet or exceed the legislative thresholds and identifies key future state privacy considerations to move The City's current privacy program into closer alignment with international privacy standards such as the *General Data Protection Regulation* ("GDPR"). In response to part (b) of the Notice of Motion:

- Attachment 1 details a Privacy Framework 2019 – 2021 Workplan for Council's consideration, and includes The City's participation in the Future Cities Canada initiative to develop and leverage data governance to support a Smart City, as well as design and test a data governance framework that can be used for future data initiatives;

- Attachment 6 provides a privacy vision and principles for The City that reinforce and build upon the purposes set out in the *FOIP Act* and will form the basis of public engagement in 2020 with citizens, organizations and privacy experts to provide input on this vision and principles to help shape The City's strategic privacy framework; and

- Attachment 7 provides results from open source research regarding a comparison of various Chief Privacy Officer roles and responsibility models across the public, private and global sectors. While the position titles vary across the various sectors, Attachment 7 demonstrates that the majority of the roles and responsibilities related to privacy are either already fulfilled under The City's current privacy model or will be completed as part of the work set out in the Privacy Framework 2019 – 2021 Workplan (Attachment 1).

Stakeholder Engagement, Research and Communication

Research of open data sources was undertaken to gather information about best practices related to privacy practices and Chief Privacy Officer positions. The City engaged with the University of Calgary and a representative of the Urban Alliance to review current state privacy practices, and to initiate discussions about a future state privacy framework for The City.

Strategic Alignment

This report aligns with Council's Priority of a well-run city: "Calgary's government is open, responsible, accountable and transparent, delivering excellent services at a fair price. We work with our government partners to ensure we have the tools we need".

Social, Environmental, Economic (External)

With respect to social impacts, as technology allows for greater collection of personal data, and as it changes how citizen data is being collected, used, stored, disclosed and destroyed, public concerns arise around loss of control over one's own personal information, monitoring, surveillance, tracking and third-party usage and disclosure of personal information. Such privacy concerns may impact City projects intended to improve social well-being when privacy is not part of the original project design and development. To minimize potential negative social

City Manager's Office Report to
Strategic Meeting of Council
2020 January 27

ISC: UNRESTRICTED
C2020-0039

City of Calgary Citizen Privacy Data Practices

impacts, The City regularly monitors privacy issues and industry best practices and adopts privacy practices to uphold public trust and confidence (Attachment 8).

Financial Capacity

Current and Future Operating Budget:

Through the Council Innovation Fund, Administration will seek budget to (1) secure services of an external privacy expert to conduct an audit of the current and future privacy practices at The City; and (2) to develop and implement a public engagement campaign. Citizens, privacy experts and organizations will be invited to provide feedback, through a variety of engagement means, that will then inform the development and implementation of privacy online tools to communicate more effectively about The City's privacy practices.

Current and Future Capital Budget:

There are no capital budget implications associated with this report.

Risk Assessment

Risks can arise from new technologies, upgrades to existing technologies, generation of large amounts of data by IoT devices and changes in business processes when privacy implications are not considered throughout the project. These privacy risks, as outlined in Attachment 9, can take many forms. The City mitigates privacy risks by adopting privacy practices such as those detailed in Attachment 8. Further, The City will mitigate any potential risk of losing public trust by completing a public engagement campaign on The City's proposed privacy vision and principles and will invite citizens, privacy experts and organizations to provide input to help shape The City's strategic privacy framework.

REASON FOR RECOMMENDATIONS:

This report responds to Council's direction to provide a status update by bringing forward an analysis of The City's current privacy practices and a workplan for the development and implementation of a strategic privacy framework.

ATTACHMENTS

1. Attachment 1 – Privacy Framework 2019-2021 Workplan
2. Attachment 2 – City Bylaws, Policies and Procedures
3. Attachment 3 – Access to Information and Privacy Training
4. Attachment 4 – Privacy and Smart Cities
5. Attachment 5 – Analysis of The City's Current Privacy Practices
6. Attachment 6 – Privacy Vision and Principles
7. Attachment 7 – Chief Privacy Models – Roles and Responsibilities
8. Attachment 8 – Privacy and Public Trust
9. Attachment 9 – Risk Assessment – Privacy Risks