
City of Saskatoon Internal Audit Report - Access and Privacy of Information

Table of Contents

Executive Summary	3
Background & Objectives	3
Key Strengths	3
Areas of Opportunity	4
Overall	4
Scope, Objectives, Approach	5
Phase 1: Current State Assessment	5
Phase 2: Road Map to Maturity	6
Detailed Observations and Recommendations	7
Access and Privacy Management Program Framework	7
Privacy Impact Assessment (PIA)	10
Privacy by Design (PbD)	12
Incident Management	14
Training and Awareness	17
Third Party Privacy Management	20
Appendix 1: Privacy Remediation Road Map	23
Appendix 2: Impact Assessment	26
Appendix 3: Interview List	27

1. Executive Summary

1.1 Background & Objectives

The Saskatchewan Information and Privacy Commissioner is an independent office of the Saskatchewan Legislative Assembly. It oversees three Saskatchewan statutes, which establish the access to information and privacy rights of citizens: *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP), and *The Health Information Protection Act* (HIPA). The City of Saskatoon (the “City”) is a local authority under LAFOIP and as such is responsible for following the requirements of LAFOIP relating to access to information in the custody or control of the City and the protection of individual privacy.

The Access and Privacy Officer role was established within the Records, Information and Legislative Services function of the City Clerk’s office in 2017 and this role is responsible for handling the Access and Privacy Management Program for the City. No further formal staffing exists within the Access and Privacy Management Program.

The City’s Strategic Risk Register includes Risk A&FS-9, which is a “medium” City Council risk priority and relates to the risk that “*The City may not be adequately protecting information created by or entrusted to it*”. The objective of this Internal Audit project is to review the City’s current privacy information framework and supporting policies against applicable and in-scope privacy regulatory requirements and leading practices. PwC worked with a number of key staff across a number of divisions to obtain an understanding of the following in-scope areas:

- Policy and Program Framework - including Privacy Impact Assessment and Privacy by Design;
- Breach Management;
- Training and Awareness; and
- Third Party Privacy Management.

1.2 Key Strengths

While the City is currently in the early stages of maturity with its Access and Privacy Management Program and relevant framework, with the hiring of a new Access and Privacy Officer in 2017 being a significant step, a number of key initiatives have been undertaken by the Administration to progress the Access and Privacy Management Program. These key initiatives include:

- Access and Privacy Management Program Framework that outlines a work plan to help the City to better align to *Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIP);
- Designing policies and procedures in certain key areas such as privacy and confidentiality, video surveillance, privacy breach protocols, and privacy impact assessments;
- Training and awareness campaigns including on-demand employee training opportunities; and
- Tools to assist business units implementing new projects that might impact personal information.

1.3 Areas of Opportunity

To further enhance the Access and Privacy Management Program, there are a number of observations and recommendations within this report, the key themes of which are as follows:

- **Privacy Program Framework** - Appointing and training privacy champions in each division to become liaisons between their division and the Access and Privacy Office.
- **Privacy Impact Assessment** - Formalizing and implementing tools to assist in the identification and analysis of privacy risks.
- **Privacy by Design** - Incorporating elements of Privacy by Design into the City's strategy to ensure that all privacy implications and risks are considered throughout the design, build and implementation stages of relevant City-wide projects and initiatives.
- **Breach Management** - Enhancing breach protocols by defining roles and responsibilities of all involved parties and also specifically indicating process for breaches of both employee and citizen information. Aligning processes for IT security risk management and breach reporting with the Privacy Breach Protocol, along with aspects of corporate security.
- **Training and Awareness** - Working alongside other City divisions and departments, enhancing the training and awareness program to ensure that all staff are fully aware of the Access and Privacy Management Program and its strategy to protect the privacy of the City's information.
- **Third Party Privacy Management** - Enhancing third party privacy management to mitigate potential third party privacy risks.

1.4 Overall

The City has made positive progress in recent years in terms of better establishing the foundation of its Access and Privacy Management Program and building on that foundation during 2017 and 2018, as outlined by the strengths identified throughout this report. In order to continue to build on that foundation and make progress with its current initiatives, the Access and Privacy Management Program should consider the recommendations within this report to supplement its currently planned activities. Implicit in a number of the recommendations is the acknowledgement that there are currently limited dedicated resources at the disposal of the Access and Privacy Management Program, and in order to implement some of the recommendations within the report in a fulsome manner additional resource needs may be identified by the Access and Privacy Management Program.

2. Scope, Objectives, Approach

Scope

The City's Strategic Risk Register includes Risk A&FS-9, which states "*The City may not be adequately protecting information created by or entrusted to it*". The objective of this Internal Audit project is to: a) review the City's current privacy information framework and supporting policies against applicable and in-scope privacy regulatory requirements and leading practices in order to allow for identification of root causes that may negatively impact risk mitigation activities of the Privacy Management Program; and b) identify improvement opportunities to align the information management lifecycle with applicable privacy regulatory requirements and good practices.

Risk A&FS-9 outlines examples of potential root causes such as:

- Lack of understanding of what information is confidential/personal;
- Absence of policies that govern collection, use, creation and storage of information;
- Inadequate information security measures; and
- Intentional/unintentional breach of information security measures or release of information.

Key in-scope areas related to the work conducted within this project include:

- Policy & Program Framework including Privacy Impact Assessment, Privacy by Design;
- Breach Management;
- Training and Awareness; and
- Third Party Privacy Management.

Areas that were out-of-scope for the work conducted within this project include:

- Records management;
- Cybersecurity;
- Access to information requests; and
- Testing operational effectiveness of controls in place.

Objectives & Approach

Our overall approach to assess the current state of the City's Privacy of Information framework and policies and to provide the City with recommendations for improvement is as follows:

Phase 1: Current State Assessment

Objectives - Gain an understanding of the City's current approach to protecting information created by or entrusted to it against applicable privacy legislation (e.g., Local Authority Freedom of Information and

Protection of Privacy Act).

Approach - The key activities to the current state assessment can be summarized as follows:

- Gather and review relevant privacy documentation related to in-scope areas;
- Conduct stakeholder interviews (e.g. privacy, third party privacy management, information security);
- Identify applicable privacy, legal, regulatory and policy requirements; and
- Assess current state policies and procedures against applicable regulatory requirements.

Phase 2: Road Map to Maturity

Objectives - Identify opportunities for improvement and develop a roadmap to help the City implement the identified recommendations for overall improvement of the Access and Privacy Management Program.

Approach - The key activities to identify and prioritize opportunities for improvement were as follows:

- Identify privacy risks and recommendations for improvement and rank according to priority; and
- Develop a remediation roadmap to mitigate identified risks according to a risk ranking scheme.

3. Detailed Observations and Recommendations

3.1 Access and Privacy Management Program Framework

Category #1: Access and Privacy Management Program Framework

Strengths

- The City has implemented the Access and Privacy Management Program Framework 2017 - 2020 to act as a coherent and comprehensive approach to corporate access and privacy management. This documented plan outlines a need for privacy staff in order to implement new policies and technology and also to update current processes and control, and includes a four-year work plan of tasks that are to be completed for each year such as, developing:
 - a Privacy Breach Protocol (completed in 2017); and
 - a Standard Operating Procedures for Managing Access to Information Requests (completed in 2018).
- The City has continued to update its policies to better align with its analysis of LAFOIP.
- The City has implemented a communication toolkit to assist the Access and Privacy Office in awareness campaigns to the entire City and to help provide privacy-related information to all staff. During the year, the Access and Privacy Office distributed a number of informative materials across the City to increase awareness for the Access and Privacy Office and the policies in place. In addition to this, the Access and Privacy Office held a Privacy week and updated the SharePoint page to include information for employees on an ongoing basis. The City is also planning to hold a session in 2019 to assist City staff in understanding applicability of the privacy standards to their roles.
- The Access and Privacy Office has had meetings with other municipalities in Saskatchewan to assist with information sharing and industry good practices.
- The City Clerk's Office, in consultation with the City Solicitor's Office, monitors changes in legislation. Updates to legislation are considered when developing Privacy and Confidentiality Policy and Procedures.

Observation (F1):

The City has limited resources available to implement and support its Access and Privacy Management Program. This includes formally or informally appointed privacy champions to liaise between the Access and Privacy Office and the City's various divisions and departments.

Risk (F1):

Without sufficient resources, privacy initiatives may not be executed regularly/consistently, resulting in decreasing privacy awareness throughout the City and updates to privacy legislation not thoroughly communicated across different departments/stakeholder groups.

Impact: 2 – Medium

Recommendation (F1):

Consider appointing delegates or departmental/divisional privacy champions who would liaise between the various departments/divisions of the City and the Access and Privacy Office. This could be monitored and reported upon a quarterly basis and through annual self-attestation to ensure that the Access and Privacy Office has visibility and is able to address any inconsistencies with the City’s privacy strategy.

The Access and Privacy Office should work with Human Resources, the Administrative Leadership Team and Senior Management Team to review impacts, assign roles and additional workloads for privacy champions. This includes assessing team maturity levels for privacy related tasks, delegation of tasks and enhancing privacy awareness (See 3.5 Training and Awareness).

Delegates or departmental/divisional privacy champions would need to have this added responsibility be a part of their annual reviews. These individuals would be on the distribution list for new updates to applicable laws and regulations. Training from the Access and Privacy Officer would be offered to these individuals annually in order to learn about new additions and changes to privacy policies and procedures, and this training should address recognition of privacy events as well as the duty to report breaches. Finally, these individuals would also provide a more formal mechanism to alert the Access and Privacy Office to projects which could impact privacy and would be a liaison for conducting privacy impact assessments and assisting in supporting breach management.

Observation (F2):

Updates to privacy policies and procedures may not be communicated to all employees of the City’s various departments and divisions. This is partly a function of the limited dedicated resources available to the Access and Privacy Office and partly a function of the current tools available and being utilized for communications.

Risk (F2):

Without sufficient communication, City staff may not be aware of changes to privacy policies leading to the incorrect application of policies to privacy-related matters.

Impact: 3 – High

Recommendation (F2):

To further awareness, in addition to having privacy policies and protocols accessible to all staff, consider holding webinars or lunch and learns. They should be used as another platform to educate staff about any changes to policies/procedures that may affect the handling of personal information.

Communications regarding updated privacy policies should be made to employees immediately after changes are approved and at least on an annual basis thereafter.

Consider engaging the Communications team to locate new opportunities, including “News Items” on the internal SharePoint site to introduce and reinforce new policies and procedures, as well as any updates to such documents. Work in collaboration with Human Resources to track employee access to new/existing policies, as well as tracking employee attestation. This employee attestation could bring heightened employee awareness to the potential consequences for non-compliance by being done either on an annual basis or whenever there are significant updates to policies. Consider leveraging the learning management system to assist with tracking of employee attestation, with this potentially only being mandatory for employees that have access to certain levels of personal information.

The Access and Privacy Office should work with Human Resources to keep track of employee acknowledgement in circumstances where policies or procedures are updated and/or training has been provided.

3.2 Privacy Impact Assessment (PIA)

Category #2: Privacy Impact Assessment (PIA)
Strengths:
<ul style="list-style-type: none"> The City has implemented a pre-PIA and PIA for application by business units in consultation with the Access and Privacy Officer to ensure that they are assessing the privacy risks around projects and determining whether the involvement of the Access and Privacy Office is required. The involvement of the Access and Privacy Office is always required for the PIA process. The PIA also includes a risk mitigation approach that addresses the mitigation strategies that will be implemented to manage privacy risks. In addition, the risks will be assessed with the likelihood (rare, unlikely, likely or certain) of the privacy impact risk occurring and the degree of the impact to privacy (negligible, moderate, major or critical) on individuals and/or the City.
Observation (P1):
The risk rating mechanism within the PIA incorporates the likelihood for the associated risks and the potential impact on the City. However, additional clarity could be incorporated to address how new or changed risks to personal information are re-visited on an annual basis and updated accordingly. There could also be additional clarity regarding any escalation processes to address potential risk areas.
Risk (P1):
By not having a consistent process to re-evaluate the privacy risk of new/ongoing projects, risks may be left unidentified or unmitigated. Delayed, ineffective and/or reactive risk management and breach remediation activities may result.
<i>Impact: 2 - Medium</i>
Recommendation (P1):
At least annually, the City should revisit new or changed risks to personal information and develop/update responses to such risks. An escalation process should be incorporated to address risks to personal information handling practices that are defined within the PIA tool.
Observation (P2):
The City would benefit from a formal mechanism to review projects to assess privacy controls and their effectiveness after projects are implemented.
Risk (P2):
Without a formal mechanism to review projects and assess the effectiveness of privacy controls post-implementation, individuals may revert to privacy-lacking protocols after implementation and therefore negatively impact the protection of personal information.
<i>Impact: 2 – Medium</i>

Recommendation (P2):

The City should consider implementing a checklist of items that departments and divisions must observe at key checkpoints of a project to ensure that privacy controls are being maintained throughout the project. This would include determining whether:

- the types of personal information collected has changed from the initial assessment performed;
- the personal information use cases have changed; and
- any new third parties have been added that were not initially evaluated for privacy.

The Access and Privacy Office, in collaboration with project managers, should consider implementing spot checks on newly implemented projects to ensure they are meeting privacy controls. Alternatively or additionally, the Access and Privacy Office could institute random selection of some percentage of projects for privacy review, which will encourage compliance with the requirement to conduct PIA's and to adhere to the mitigation activities identified in them.

3.3 Privacy by Design (PbD)

Category #3: Privacy by Design (PbD)

Observation (D1):

The City leverages PIAs and Pre-PIA policies and procedures to assist with privacy implementation into its different projects. However, it appears that there are no formally defined and documented PbD policies and procedures in place.

PbD includes embedding the 7 foundational principles into the design and implementation of systems and technologies:

1. Proactive not Reactive, Preventative not Remedial – Including taking of proactive rather than reactive measures to anticipate and prevent privacy invasive events before they occur.
2. Privacy as the Default Setting – To deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy –it is already built into the system, by default.
3. Privacy Embedded into Design – Ensuring that privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons, after the fact.
4. Full Functionality – Positive-Sum, not Zero-Sum – Providing a full integration of privacy and security into the design, and avoiding the pretense of false dichotomies, such as privacy vs. security.
5. Full Lifecycle Protection – End-to-End Security - Security measures are essential to privacy, from start to finish, to ensure that all data are securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion.
6. Visibility and Transparency – Including making sure that there is transparency with the users and individuals whose personal information is collected are made fully aware of the personal data being collected, and for what purpose(s).
7. Respect for User Privacy – Keep it User-Centric - Including providing measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Using PbD, at the time of new project or initiative design, project owner(s) must define the following:

- Business requirements;
- Privacy principles that are relevant to the project and/or initiative; and
- Extent to which the privacy principles are reflected in an acceptable privacy design.

Risk (D1):

By not enabling PbD, the City may not be assessing risks in its data processing activities when initiating new projects. This could include an increased collection and processing of personal information and potential mishandling of personal information. PbD and PIA processes reduce the risk of project cancellation or re-work to address compliance, and their absence increases risks of cost overruns.

Impact: 2 - Medium

Recommendation (D1):

Develop a PbD policy and procedure to help ensure that all privacy implications and risks are considered at the design stage in all projects and initiatives that would provide guidance for to developers in the design and implementation phases of development. In addition, it is also highly recommended that privacy remains a key consideration through the entire project lifecycle.

As noted above in the PIA comments, random selection of some percentage of projects for privacy review could encompass review of projects to ascertain whether PbD principles were being followed in the design and implementation of systems and technology.

3.4 Incident Management

Category #4: Incident Management
Strengths:
<ul style="list-style-type: none"> • Breach protocols have been created, approved and distributed City-wide. The protocols contain guidelines to assist divisions and departments in the case a breach has been identified. • Protocols indicate that the Access and Privacy Office would be involved in any incidents that may occur. If required, the Privacy Commissioner would be contacted. • The City is developing a process map to aid in streamlining the incident management process.
Observation (I1):
<p>It was noted that citizens act as one avenue of breach discovery, by emailing or calling through the City Webmaster system with notification of a breach. The forms submitted by citizens are used by the City for internal investigations and are then retained within the breach investigation file in a protected folder maintained by the City Clerk’s office. Other avenues of breach discovery include IT and individual departments.</p> <p>It was noted that the City has developed a privacy breach protocol to address potential breaches impacting personal information. This included steps that should be taken in the event of a breach. However, we noted that processes to address a breach are not always consistent between departments.</p> <p>It was noted that IT has its own mechanisms for identifying and responding to information security threats, while other business units are responsible for identifying operational issues. IT has its own central repository that is used for breach record keeping, however it is not clear whether this is also utilized by the Access and Privacy Office.</p> <p>The City’s Privacy Breach Protocol includes a requirement to report privacy breaches to the City Clerk (or Designate) immediately in order to initiate coordination of the next steps in the Privacy Breach Protocol by the Access and Privacy Officer, including notification to the Office of the Information and Privacy Commissioner. However, improved communication of this protocol is recommended to clarify to all divisions and departments what the required reporting requirements are.</p>
Risk (I1):
<p>A lack of documented and defined protocols can lead to inconsistent application of procedures across the City and further potential mishandling of information. Inconsistent incident management processes and undefined roles and responsibilities could result in mishandling breach responses and not notifying affected individuals or regulators.</p> <p><i>Impact: 2 - Medium</i></p>
Recommendation (I1):
<p>To ensure that team efforts are used wisely and there is clear ownership of tasks for the remediation of an incident, the City should consider updating its incident management policies and procedures. This would include defined roles and responsibilities between departments/divisions, the Access and Privacy Office, IT and third parties as well as the following:</p>

- Escalation protocols - i.e., when to contact the Access and Privacy Office and IT in the event of a suspected breach;
- Definitions of evidence that needs to be preserved (i.e. forensic, legal, etc.); and
- Responsibility for notifying affected individuals, third parties and regulators.

The Access and Privacy Office should continue to work directly with IT to understand how IT is engaged in breach management, as well as ensure where IT is not engaged in breach (as where physical files might be lost or misplaced, or an email containing sensitive information is mis-sent). This would include the division of roles and responsibilities, policies and procedures and at what point the Access and Privacy Office is engaged.

The City should implement a centralized breach management record keeping system to facilitate in the record keeping of breaches that have occurred within the City. We understand that IT leverages a record keeping system and this recommendation is to ensure that IT and the Access and Privacy Office fully incorporate the following into breach record keeping:

- Record retention schedule that is aligned with the City’s record retention policy;
- Listing of which information should be captured;
- Assigned roles and responsibilities; and
- Access controls.

Observation (I2):

The City would benefit from formalized tabletop exercises for privacy incidents and/or breaches.

Risk (I2):

Without a practiced and tactical understanding of how to react in a real or suspected breach scenario, employees may inadvertently slow or hamper the breach reporting or remediation process, or worsen a breach and how it might be perceived by affected stakeholders.

Impact: 2 - Medium

Recommendation (I2):

The City should consider designing a formalized table-top training strategy to address privacy and breach incidents. It is important to identify all potential stakeholders that would need to take part in training, including individuals from Privacy, Human Resources, Customer Service, Finance, Payroll, and IT.

When designing privacy table-top exercises, it is important to develop multiple scenarios that are straightforward and easy to understand. Examples include a lost laptop with personal information, personal information emailed to the wrong person, or a server infected with malware. It is also important to identify what privacy laws or industry best practices may be affected during the exercise (e.g., mandatory breach notification).

Once implemented, conducting annual simulation of table-top training exercises and documenting the results is considered best practice. Simulation exercises should incorporate privacy champions and/or department leads to facilitate a streamlined incident management approach across departments.

Observation (I3):

The City would benefit from a defined and documented process to identify the steps that would be taken in the case that a breach impacts employee's personal information. Although we noted that the City would take the same steps outlined within the Privacy Breach Protocol, there are additional measures to consider that specifically relate to notifying employees affected by privacy breaches. It is important to ensure that breaches pertaining to employee information are handled appropriately and they may require additional steps pertaining to notification and handling. The Breach Protocol should address those differences and similarities between the data types.

Risk (I3):

Breaches pertaining to employee information may not be dealt with in a timely and consistent matter and/or negatively impact employee morale.

Impact: 2 – Medium

Recommendation (I3):

Breach Protocol should specifically indicate that the procedures relates to both breaches of citizens personal information and employee information. In consultation with Human Resources, the City should consider developing additional consideration specifically for notifying affected employees. This could include the following measures:

- Consider if employees are unionized and if notification to union representatives is required according to the terms of the relevant collective agreements and additional requirements.
- When notifying employees, include the following details:
 - o circumstances of the breach;
 - o day on which, or period during which, the breach occurred;
 - o personal information that is the subject of the breach;
 - o steps the City has taken to reduce the risk of harm that could result from the breach;
 - o steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
 - o contact information that the affected individual can use to obtain further information.
- Consider hosting sessions where managers and directors can speak directly with their staff regarding the breach – including answering any questions and providing additional clarity.

3.5 Training and Awareness

Category #5: Training and Awareness
Strengths:
<ul style="list-style-type: none">• Privacy training is provided by the Access and Privacy Officer on an on-demand basis and is provided to Records and Information Coordinators on a quarterly basis. A number of staff across the City have received privacy and access training, which helps them to identify and manage personal information.• The Access and Privacy Office held a Privacy Week initiative in 2018.• The Code of Conduct and Confidentiality Oath signed by new employees contains sections relating to privacy. The Code of Conduct and Confidentiality Oath is added to the employee file during onboarding. Implementation for all existing employees began in June 2018 and it will be required for all new employees.• A SharePoint site has been initiated to contain all enacted privacy related policies and procedures, as well as the PIA tool and guideline document, along with privacy education information.• The City is working in consultation with Human Resources to enhance its privacy training and awareness activities for 2019 through developing out its retention policies and procedures, implementing an online training portal and enhancing the onboarding and ongoing training program.
Observation (T1):
The City would benefit from a formal privacy training and awareness program for employees across different divisions and departments. General employee training is provided to all employees upon hire, however, the training does not include privacy content. The Access and Privacy Office does deliver privacy training to employees on an adhoc basis and Records and Information Coordinators receive training as part of their onboarding that includes privacy elements. IT staff generally receive no formal training in this area, however some IT staff will receive training around privacy in its regard to security. Some staff in this role are actively trained on how to determine what constitutes a breach.
Risk (T1):
Employees may not fully understand their privacy and security responsibilities including, for example, who to contact in the event of a breach. A lack of awareness can create new, and enhance existing, privacy and security vulnerabilities for the City.
<i>Impact: 2 - Medium</i>
Recommendation (T1):
The City should consider developing a mandated privacy training and awareness program to promote awareness of privacy across the City and allow the City to fully meet its legislative privacy compliance standards. Specific training should be developed and provided to select employees depending on their assigned roles and responsibilities. Some best practices with respect to training and awareness include:

- Having employees participate in privacy training on an annual basis and including a quiz with a minimum passing score to test employee knowledge;
- Tracking of employees who have completed the privacy training and employees who have not – this should be completed in collaboration with Human Resources;
- Assessing job levels and what access employees have to personal information – all employees should receive the standard training, however additional training should be tailored to roles and responsibilities; and
- Making the privacy training program mandatory for all new employees before they access personal information and periodically thereafter.

To maintain awareness, privacy updates and refreshers can also occur via monthly newsletters and/or bi-weekly social newsletter "Social Links", if appropriate. These updates can be sent by the Access and Privacy Office or by divisional/departmental privacy liaisons.

In addition, the City should consider continuing with its initiatives such as the Team Talk, Supervisor privacy curriculum integration, updates to the SharePoint site and addition of the “News Feature”.

In consultation with Human Resources, Administrative Leadership Team and the Senior Management Team, determine if additional training is required for “Privacy Champions” (see 3.1 Access and Privacy Management Program Framework).

Observation (T2):

Staff may have difficulty understanding the City’s privacy strategy, including what is confidential information and what can and cannot be shared. The City has limited guidance on what information should be stored, for how long and how information is to be reviewed to ensure that it is still relevant.

Risk (T2):

Employees may not fully understand their privacy and security responsibilities including, for example, who to contact in the event of a breach. A lack of awareness can create new, and enhance existing, privacy and security vulnerabilities for the City.

Impact: 2 - Medium

Recommendation (T2):

The City should consider working with individual departments and divisions to develop step-by-step guidelines/procedures to assist with daily responsibilities and avoid unauthorized collection, use and disclosure of personal information (e.g., create a “Job Aid” for securing the transmission of sensitive information via email).

The City should also consider enhancing policies by specifically detailing all information that is considered “personal information”. These types of data should have a termination date from City systems and also have a frequency for review. This will provide comfort to the City that the risks related to the storage of confidential information is reduced to its lowest, required state.

Observation (T3):

The City would benefit from more fulsome training for its staff with respect to existing policies and procedures. A simple example of this could be lack of awareness with respect to the City's Acceptable Use and Mobile Device Policy.

Risk (T3):

City staff may not be aware of existing policies and procedures and/or may not be using them in alignment with City's personal information handling practices.

Impact: 2 – Medium

Recommendation (T3):

The City should consider evaluating its training program and ensure that existing policies and procedures are covered including acceptable use protocol / mobile use protocol. Consequences of non-compliance should be communicated. Employees should review and sign off on the policies on hire and annually.

The City should leverage its existing "News Feed" on the SharePoint website to communicate existing policies and procedures and any updates to such documents going forward. Work in consultation with Human Resources to monitor which staff have reviewed the documentation and collect attestations. Consider leveraging the learning management system to assist with tracking of employee attestation, with this potentially only being mandatory for employees that have access to certain levels of personal information.

3.6 Third Party Privacy Management

Category #6: Third Party Privacy Management
Strengths:
The City has recently implemented a new procurement policy. Although the policy itself does not specifically address items related to privacy, there is an opportunity for the Access and Privacy Office to engage in the process of ensuring that appropriate third party privacy management activities are incorporated.
Observation (V1):
The City would benefit from a formal review of its third party privacy practices prior to onboarding. During the third party pre-award phase, IT is involved in reviewing third party practices to determine whether third party policies align with the City's security standards and controls. This has to be approved before access to systems is provided to third parties. However, the Access and Privacy Office does not currently conduct a privacy review of third parties before they are onboarded.
Risk (V1):
Without a proper onboarding program, third parties with inadequate privacy programs might have access to the City's information, which creates exposure to the City and creates vulnerabilities, as the City would still be accountable for data protection. <i>Impact: 2 – Medium</i>
Recommendation (V1):
The City should developed a tiered approach to assist with third party privacy management, including onboarding. This tiered approach would incorporate a level of risk based on the type of access the third party has and the type of information it processes. For example consider the following: Tier 0: <ul style="list-style-type: none">• No data is being stored, held or processed by the Supplier or their systems. Personal information is limited to e-mail contact information of City employees Tier 1: <ul style="list-style-type: none">• Any data being processed or maintained that falls within the City's Data Classification of "Public". The information being collected from individuals consists solely of contact information (name, address, phone, e-mail). Tier 2: <ul style="list-style-type: none">• Any data being processed or maintained that falls within the City's Data Classification of "Internal Use Only".• If "Confidential" or "Private" data is being collected then it is being collected solely on the account of the Supplier and such personal information is being provided directly by individuals to the Supplier.

Tier 3:

- Any data being processed or maintained that falls within the City’s Data Classification of “Confidential”, or “Private”.
- Such personal information is being provided directly by the individual to the City, the Supplier, other partner or other source with the stated purpose of providing such personal information to the City.

The third party onboarding practices should be relevant to the Tier Level the third party applies to. For third parties in Tier 2 or Tier 3, the City should perform an evaluation over the third party’s privacy policies and determine whether any revisions would need to occur before services are transacted.

Third Parties can be assessed against a set of criteria set out by the Access and Privacy Office and Materials Management based on relevancy and risk. The criteria would include assessing the level of security of the third party, assessing the number of third party staff that will be involved, and if there will be any sub-contractors employed by the third party.

Observation (V2):

The City would benefit from formal third party monitoring within a formal third party management program, including formalized annual reporting (e.g., SOC reports) or regular auditing of privacy practices of its third parties, where appropriate for the nature of the risks associated with the data being managed or held by the third party.

Risk (V2):

Third parties might process City information in non-compliance with regulations or with the City’s internal policies and procedures. Third parties working in alliance with the City are seen as an extension of the City through the data processing activities, which could have negative implications on the City in the event of non-compliance or a breach.

Impact: 2 - Medium

Recommendation (V2):

The City should consider the implementation of a third party privacy management program that is based on the tiered approach. If the third party processes personal information, then the management program should incorporate the following:

- An annual privacy audit to assess the level of privacy control effectiveness. The results of the audit can then be used by the City to assess gaps as the program continues to grow and evolve.
- A formal third party privacy risk assessment, in conjunction with a security or threat risk assessment on third parties, to assess, evaluate and document risks in third party organizations.
- A review of existing third party agreements to ensure compliance with the strategy on sharing personal information; and
- Other mechanisms, for lower level of risks, may include self-certification, periodic reviews less formal than audits, or questionnaire-based assessment.

The incorporation of third party management into privacy awareness training for employees will assist in understanding what information can be disclosed to third parties, what appropriate agreements look like and how to comply with legal and business requirements. Conducting a periodic review of all third parties to identify third parties that no longer have a business relationship with the City and remove access is an important privacy component of a third party privacy management program.

Observation (V3):

The City would benefit from a formalized and defined strategy to off-board its third parties that process and store personal information. Although the City Clerk's office monitors this from a contractual perspective, there are no mechanisms to validate that data is returned or deleted upon relationship termination (e.g., certificate of destruction provided to the City by third parties) or that any potential access is shut off.

Risk (V3):

Without a formalized off-boarding process, third parties may continue to have access to City systems or continue to store and utilize personal information in their possession after the relationship ends. In addition, third parties could have inappropriate access to City systems and information.

Impact: 2 – Medium

Recommendation (V3):

The City should define, document and formally implement a third party offboarding program. This would include a checklist of items to be completed during the off-boarding of third parties, including generating exit documents, obtaining a certificate of data destruction, and notifying relevant staff, department heads and IT in order to begin de-provisioning user logins. The City should work to develop out this offboarding program based on the tiered approach.

Observation (V4):

The third party privacy management process, including management, onboarding and offboarding, would benefit from more formal definition and documentation for a consistent City-wide approach.

Risk (V4):

The City could be at an increased risk of privacy breaches as a result of an inconsistent approach to third management, including the onboarding to offboarding of.

Impact: 2 - Medium

Recommendation (V4):

The City should consider the implementation of a City-wide policy that dictates the City's position on third party privacy management. This should incorporate a tiered approach that is consistent with the level of risk based on the type of access the third party has and the type of information it processes. This will ensure that procedures are performed consistently, upholding City values for external parties. The policy should include a clear definition of the roles and responsibilities for the Access and Privacy Office, IT, Materials Management and individual divisions and departments for interacting with third parties, including checklists and procedures for onboarding, third party maintenance and offboarding.

Appendix 1: Privacy Remediation Road Map

Roadmap: Key activities by Privacy Observation	Timeline				
	Level of Effort	Short Term	Short to Mid Term	Mid to Long Term	Long Term
High Priority based on Impact Rating and Level of Effort <ul style="list-style-type: none"> F2 - Develop a mechanism to communicate updates to privacy policies and procedures internally 	Low	Completed			
Medium Priority based on Impact Rating and Level of Effort <ul style="list-style-type: none"> F1 - Appoint delegates/privacy champions to act as liaisons with the Privacy Office P1 - Revisit new or changed risks to personal information at least annually and incorporate an escalation process into the PIA tool P2 - Implement checklist for use during project checkpoints to review projects and assess the effectiveness of privacy controls D1 - Develop PbD policy and procedure to ensure privacy implications are considered at the design stage in all projects and initiatives 	Medium				
	Medium				
	Medium				
	High				

Timeline

Roadmap: Key activities by Privacy Observation

Medium Priority based on Impact Rating and Level of Effort

- **T1** – Develop a mandatory privacy training and awareness program
- **T2** - Develop tailored privacy procedures to assist departments and divisions in their day-to-day responsibilities in privacy management to avoid unauthorized collection/use/ disclosure of personal information
- **T3** – Evaluate privacy training program to ensure key policies and procedures are included (e.g., acceptable use and mobile use protocols)
- **V1** - Formally define and implement a third party onboarding program that incorporates privacy and security of personal information
- **V2** – Enhance the third party privacy management program to incorporate privacy and security of personal information
- **V3** - Formally define and implement a third party off-boarding program to address privacy and security of personal information.
- **V4** – Implement a City-wide policy on third parties to address the City’s position on third party privacy program management

	Level of Effort	Short Term	Short to Mid Term	Mid to Long Term	Long Term
	High				
	High				
	Medium				
	High				
	High				
	High				
	High				

Roadmap: Key activities by Privacy Observation






Timeline

Medium Priority based on Impact Rating and Level of Effort

- **I1**- Enhance breach protocols to include roles and responsibilities and develop a centralized breach management record system
- **I2** - Design a formalized table-top training strategy to address privacy and breach incidents
- **I3** - Enhance breach protocols to indicate procedures related to breaches of citizen and/or employee information

Level of Effort	Short Term	Short to Mid Term	Mid to Long Term	Long Term
Medium				
High				
Medium				

Appendix 2: Impact Assessment

Observation Rating	Assessment Rationale
Critical (4) 	An observation for which the exposure arising could have a: <ul style="list-style-type: none"> • Critical impact on operational performance [<i>e.g. resulting in inability to continue core activities for more than two days</i>]; or • Critical monetary or financial statement impact; or • Critical breach in laws and regulations that could result in material fines or consequences; or • Critical impact on the reputation or brand of the organization which could threaten its future viability [<i>e.g. high-profile political and media scrutiny i.e. front-page headlines in national press</i>].
High (3) 	An observation for which the exposure arising could have a: <ul style="list-style-type: none"> • Significant impact on operational performance [<i>e.g. resulting in significant disruption to core activities</i>]; or • Significant monetary or financial statement impact; or • Significant breach in laws and regulations resulting in significant fines and consequences; or • Significant impact on the reputation or brand of the organization [<i>e.g. resulting in unfavourable national media coverage</i>].
Medium (2) 	An observation for which the exposure arising could have a: <ul style="list-style-type: none"> • Moderate impact on operational performance [<i>e.g. resulting in moderate disruption of core activities or significant disruption of discrete non-core activities</i>]; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations resulting in fines and consequences; or • Moderate impact on the reputation or brand of the organization [<i>e.g. resulting in limited unfavourable media coverage</i>].
Low (1) 	An observation for which the exposure arising could have a: <ul style="list-style-type: none"> • Minor impact on operational performance [<i>e.g. resulting in moderate disruption of discrete non-core activities</i>]; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organization [<i>e.g. resulting in limited unfavourable media coverage restricted to the local press</i>].
Other 	Internal Audit functions commonly have an ‘other’ category whereby they would raise an observation that does not fall into any of the above categories for one reason or another. These could be observations that are out of scope of the audit, but internal audit wanted to document or discuss, or observations with a nominal expected exposure. These could be verbal observations or those documented with no associated rating.

Appendix 3: Interview List

Name	Division	Title
Wenda Atkinson	City Clerks	Access and Privacy Officer
Sarah Sliva	City Clerks	Corporate Records Manager
Kim Matheson	Strategic and Business Planning	Director
Scott Eaton	Materials Management	Director
Michelle Tetreault	Employment & Total Compensation	Manager
Cindy Yelland	Legal Services	Director
Paul Ottmann	Information Technology	Director
Kevin Shewchuk	Information Technology	PMO
Jazz Pabla	Information Technology	Technical Infrastructure Manager
Carla Figg	Service Saskatoon	Customer Service Manager

This document has been prepared only for the City of Saskatoon and solely for the purpose and on the terms agreed with you. We accept no liability (including for negligence) to anyone else in connection with this document.

© 2018 PricewaterhouseCoopers LLP, an Ontario limited liability partnership. All rights reserved. PwC refers to the Canadian firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.