Administrative Response and Timelines – Internal Audit Report – Access and Privacy of Information

Recommendation
That the report of the City Clerk, dated March 11, 2019, be received as information.

Topic and Purpose

The purpose of this report is to provide the Administration's overall assessment and response to the recommendations contained in the Internal Auditor's report on "Access and Privacy of Information".

Report Highlights

1. The audit report identifies 15 recommendations in key priorities areas to support the work of the Access and Privacy Management Program to move it towards a more mature program with improved privacy management processes and procedures.
2. The Administration will focus on communication, education and awareness opportunities as a first step to address related aspects of all privacy management recommendations. Other aspects of the recommendations that are reasonable and feasible within existing resources will be implemented beginning in 2019.
3. A collaborative approach will be explored with strategic partners within the City, including IT, HR and Supply Chain Management, to bring forward a plan to address both privacy and security-related aspects of privacy management. This will include identification of resource requirements.
4. The Administration will work towards implementing and updating processes to reflect best practices.

Strategic Goals

This report and audit support the Strategic Goal of a Culture of Continuous Improvement and the priority of protecting the privacy of individuals as required under *The Local Authority Freedom of Information and Protection of Privacy Act* and to do so in the most cost effective and reasonable manner possible.

Background

The City of Saskatoon (the "City") Strategic Risk Register contains risk A&FS-9, which states that "The City may not be adequately protecting information created by or entrusted to it". This risk was identified as a medium priority for City Council and, based on the risk rating exercise conducted by the Corporate Risk Committee, has a residual risk severity of 3.6 (which represents "medium" residual risk).

An audit of the City's processes with respect to the City's current privacy framework and supporting policies and procedures was in included in the approved 2018 Internal Audit Plan. The focus was to identify improvement opportunities to align the information management lifecycle requirements with applicable privacy regulatory requirements and good practices for privacy risk management.

The Statement of Work provided by PricewaterhouseCoopers LLP (PwC) for the Access and Privacy of Information Audit was approved by the Standing Policy Committee on Finance on August 7, 2018.

Report

Internal Audit Report Recommendations

The Access and Privacy of Information Audit Report contains 15 recommendations relating to the improvement for privacy of information management for the City. As noted in the report, the recommendations identify opportunities for improvement in key areas including:

- Appointing and training privacy champions in each division to become liaisons between their division and the Access and Privacy Office;
- Formalizing and implementing tools to assist in the identification and analysis of privacy risks;
- 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;
- Enhancing privacy breach protocols by more clearly defining roles and responsibilities of all involved parties and also specifically indicating processes for breaches of both employee and citizen information and aligning processes with IT security risk management and breach reporting with the Privacy Breach Protocol, along with aspects of corporate security;
- 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; and
- Enhancing third party privacy management to mitigate potential third party privacy risks.

Education, Awareness and Communication and Implementation of Initial Enhancements

As identified prior to the audit and as highlighted throughout the recommendations in the audit, a major focus for 2019 will be on providing opportunities to increase awareness and to educate and train about the City's access and privacy management program. The opportunities are identified in Attachment 1 in relation to key themes identified in the audit report. Those initiatives that can be explored within existing resources will be focused on in the first phase. There is currently one full-time FTE,

with some assistance at the management level, to support the City's Access and Privacy Management Program.

As identified in Attachment 1, there are some aspects of the identified opportunities that are already underway, including automation of the privacy impact assessment tool and inclusion of a risk rating tool, as well as completion of an internal SharePoint site to provide information about the program and related policies to all employees. Further communication opportunities to highlight this information will be pursued.

Further resource requirements will be reviewed as part of the 2020-2021 and future business planning and budget processes. This will include identification of FTE, technical, and other related resource requirements to implement the recommendations in the audit and support the work of the Access and Privacy Management and the Corporate Records and Information Management Programs, which are administered by the City Clerk's Office. These are related programs which impact access and privacy management for the City.

A Collaborative Approach to Privacy and Security Management

The City Clerk's Office will be working with strategic partners including IT, Human Resources and Supply Chain Management, as well as other divisions and departments across the City, to develop a collaborative approach for privacy and security management for the City. Further reporting will occur with respect to the development of a corporate strategy for security and privacy management, as well as identifying resource requirements to address portions of the recommendations that may not be achievable within existing resources.

Implementation and Updating of Processes

To assist in more effective delivery of privacy management tools, the Administration is working with IT on the automation of the privacy impact assessment processes. Further short-term solutions for improvements to processes for privacy management have been identified in Attachment 1 and will be pursued as resources permit. Longer term solutions, including opportunities within an ERP system to identify and manage risk relating to third party privacy management, will be explored following implementation of that system.

The City will continue to look for opportunities to improve the way privacy of information is managed to provide for implementation of best practices, including those that can be accomplished within existing resources and those that will require a review of resource requirements relating to a collaborative and comprehensive strategy for privacy and security management.

Communication Plan

An internal communication plan will be developed to share the Access and Privacy of Information Audit and roadmap with staff across the organization. The communication

plan will provide information about the direction of the Access and Privacy Management Program for the City, including training and education opportunities.

Financial Considerations
Further review will occur with respect to resource requirements and, as appropriate, will be included in the 2020-2021 and future budget submissions.

Other Considerations/Implications
There are no environmental or CPTED implications or considerations.

Due Date for Follow-up and/or Project Completion
Further reporting will occur with respect to a longer-term strategy utilizing a collaborative approach to security and privacy management, and will identify further resource requirements. A follow-up report on the status of all audit recommendations will be presented to the Standing Policy Committee on Finance in March 2020.

Public Notice
Public Notice pursuant to Section 3 of Policy No. C01-021, Public Notice Policy, is not required.

Attachments
1. Administration Response – Current Status, Next Steps and Timelines

Report Approval

Written by:	Diane Kanak, Deputy City Clerk/Records, Information and Legislative Services Manager
Reviewed by:	Wenda Atkinson, Access and Privacy Officer
	Paul Ottmann, Director of Information Technology
Approved by:	Joanne Sproule, City Clerk

Theme	#	Action/Recommendation	Current Status	Next Steps	Owner	Timeline
Privacy Program and Framework	F1	Appoint delegates or departmental/divisional privacy champions to act as liaisons with the Privacy Office	Many areas deal regularly with personal information and are in regular contact with the Access and Privacy Officer.	Work with the Administrative Leadership and Senior Management teams to increase privacy awareness across the corporation and determine the best model for bringing privacy matters to the forefront.	City Clerk's Office	Begin Q2 2019
	F2	Develop a mechanism to communicate updates to privacy policies and procedures internally Work with HR to track employee attestation regarding policies and procedures.	A SharePoint site has been developed that includes all policies as well as a separate site for the Access and Privacy Management Program. Employee acknowledgement of Code of Conduct and Oath of Confidentiality form part of the employee records captured in the City's approved electronic records management system (Documentum).	Work with Communications on further ways to improve internal communications to all employees about the privacy management program, including privacy policies and procedures. A newsfeed feature on the internal SharePoint site will be utilized when there are updates to the privacy management program, policies or procedures.	City Clerk's Office (in consultation with Communications)	Initial steps in place and completed. Further work on improved communications – Q3 2019
Privacy Impact Assessment (PIA)	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.	A comprehensive PIA process was introduced as a pilot in mid-2015 and formally approved in December 2015. The process was reviewed and refined in 2018, with automation of the process currently under development with assistance from IT. The corporate risk rating tool has been added to the PIA process.	Introduce the automated PIA tool, which includes identification of privacy risks, utilization of the risk rating tool, and identification of mitigation measures, and provide training, The City Clerk's Office will work with internal strategic partners to determine a mechanism for annual review, either through contract management protocols in Supply Chain Management or through the ERP system once it is implemented. Resource requirements regarding the annual review will be reviewed.	City Clerk's Office	Initial steps will be implemented Q1 2019 Begin exploration of next steps in Q2 2020.
	P2	Implement checklist for use during project checkpoints and assess the effectiveness of privacy controls.	The PIA process currently addresses identification of privacy risks at the beginning stages of a project, along with mitigation measures.	Develop a checklist to be used to provide for privacy protection and management throughout the lifecycle of projects, working with IT, Supply Chain Management and business units. As time permits, perform random audits of privacy management for projects.	City Clerk's Office	Q2 2020

Theme	#	Action/Recommendation	Current Status	Next Steps	Owner	Timeline
Privacy by Design (PbD)	D1	Develop PbD policy and procedures to ensure privacy implications are considered at the design stage in all projects and initiatives and continue through the entire project lifecycle. Implement random selection of some percentage of projects for privacy review to ascertain whether PbD principles are being followed in the design and implementation of systems and technology.	Many of the PbD principles are part of the Privacy Impact Assessment (PIA) process and the Privacy and Confidentiality Policy. Business requirements are identified as part of the Opportunity Assessment process for new projects conducted by IT and the business units.	Adjustments to the PIA tool will be reviewed where necessary to incorporate elements of PbD identified in the audit that might not currently be addressed in the PIA process, including project lifecycle management. A checklist similar to that used by IT for implementation of technology solutions through the Contract Management Protocol process will be explored with Supply Chain Management. Random selection of projects for privacy review will be explored, working with strategic partners to implement, to monitor the implementation and ongoing monitoring of privacy mitigation measures. Resource impacts and requirements will be reviewed.	City Clerk's Office and IT (regarding security aspects)	Q2 2020
Incident Management	I1	Enhance breach protocols to include roles and responsibilities and develop a centralized breach management record system.	A Privacy Breach Protocol process is in place. A security breach reporting process is also in place.	The Privacy Breach Protocol and the security breach reporting processes will be reviewed with IT to make sure the processes align and that the roles and responsibilities are clearly understood and communicated. It will also be clarified that the City Clerk or Designate is to be contacted regarding any breaches involving personal, sensitive third party and other confidential information to initiate coordination of the next steps in privacy breach management by the Access and Privacy Officer. The City's approved electronic records management system will be used for breach management records.	City Clerk's Office and IT (in consultation with HR)	Begin Q2 2019
	I2	Design a formalized table-top training strategy to address privacy and breach incidents		This will form part of the City's Access and Privacy training and education program. In consultation with IT and HR work with divisions and department to review current processes regarding breach identification and reporting and provide practical realistic scenarios that could occur in the particular business units.	City Clerk's Office (in consultation with IT and HR)	Q2 2020 and ongoing

Theme	#	Action/Recommendation	Current Status	Next Steps	Owner	Timeline
Incident Management cont'd	I3	Enhance breach protocols to indicate procedures related to breaches of citizen and/or employee information	The Privacy Breach Protocol document provides procedures related to breach of an individual's personal information, whether citizen or employee personal information.	The Privacy Breach Protocol document and process will be reviewed with HR to determine whether there are any changes required relating to handling of employee personal information. We will work towards improved communication, training and education regarding breach reporting, investigation and follow up.	City Clerk's Office (in consultation with IT and HR)	Begin Q2 2019
Training and Awareness	T1	Develop a mandatory privacy training and awareness program	Privacy training is provided upon request. Privacy information is provided to Records Coordinators within business units. Privacy awareness information for employees is provided on an internal SharePoint site.	A major focus in 2019 will be providing privacy training and awareness. In the short-term, basic information about employee responsibilities for managing personal and other confidential information will be included in new hire packages. Further exploration with HR will occur on the feasibility of including mandatory privacy awareness training as part of onboarding. RIM 101 Training will be offered starting in 2019, to include access and privacy management. We will continue to communicate through our SP site to employees about privacy management. Video and online training opportunities will be explored, along with regular monthly privacy training offerings, as resources permit. Privacy Impact Assessment (PIA) sessions will be provided to super users of the PIA program once the automated tool is available. The initial phase will include IT project leads and business relationship managers, as the IT Opportunity Assessment process connects business unit project leads to the PIA process. Opportunities to include privacy training as part of Supervisor 101 program will be pursued with HR.	City Clerk's Office (in collaboration with HR, Communications and IT and other internal strategic partners)	Begin in Q1 2019 and ongoing.

Theme	#	Action/Recommendation	Current Status	Next Steps	Owner	Timeline
Training and Awareness	T2	Develop tailored privacy procedures to assist lines of business in completing their day-to-day responsibilities	Specific training is provided to business units upon request. Privacy policies and procedures are in place on a corporate-wide basis. Processes are reviewed as time permits.	Development of business unit specific privacy processes and procedures will be implemented as resources permit.	City Clerk's Office (in collaboration with business units)	Q4 2020 and ongoing.
	T3	Evaluate privacy training program to ensure key policies and procedures are included (e.g. acceptable use and mobile use protocols) and monitor and track review and attestation by employees	The Employee Code of Conduct is in place and addresses all key policies and procedures. All employees are required to sign an acknowledgement of the Employee Code of Conduct and Oath of Confidentiality.	The Employee Code of Conduct, which includes privacy and security policies, provides the foundation for further work. Exploration of the development of mandatory online training on both privacy and security policies and procedures will be pursued with HR, IT and other security partners, along with exploration of outside consultant support for development of online training resources. A further report will be provided on a collaborative privacy and security management strategy. As noted above, tracking of employee attestations to the Employee Code of Conduct and Oath of Confidentiality is through the City's approved electronic records management system.	City Clerk's Office and IT (along with other HR and other internal strategic partners across the City)	Begin Q2 2020

Theme	#	Action/Recommendation	Current Status	Next Steps	Owner	Timeline
Third Party Privacy Program Management	V1	Formally define and implement a third party onboarding program that incorporates privacy and security of personal information	Privacy and confidentiality requirements are included as part of agreements with third parties that have access to personal or other confidential information. Those involving access to City data, are managed through IT and require Non-Disclosure Agreements, with annual reviews. This is also managed through the requirements of the Privacy and Confidentiality Policy.	In the short-term, the Privacy Impact Assessment process will continue to be used for all new projects and initiatives. Opportunities to incorporate privacy management activities in third party contractor management, including development and use of a privacy checklist and information on the Supply Chain Management SharePoint site, will be pursued with Supply Chain Management to assist business units in onboarding third party providers. In the longer term, further communication and education of the requirements of LAFOIP and the Privacy and Confidentiality Policy regarding third party privacy program management will be undertaken. Full implementation of what is proposed with this recommendation with respect to onboarding, ongoing monitoring, and off-boarding will be more feasible with the implementation of the procurement and contract management components of an ERP system, with tools to monitor, track and audit third party privacy management activities. In the meantime, the City will start to take steps to align with this best practice.	City Clerk's Office and IT (in consultation with Supply Chain Management and other divisions and departments)	PIA process is in place for all new initiatives. Will begin pursuing short-term initiatives in Q2 2020, with longer term initiatives being 18-24 months post ERP implementation of procurement and contract management modules.
Third Party Privacy Program Management	V2	Enhance the third party privacy management program to incorporate privacy and security of personal information.	As identified in V1 above.	As identified in V1 above.	As identified in V1.	As identified in V1.
	V3	Formally define and implement a third party off-boarding program to address privacy and security of personal information.	As identified in V1 above.	As identified in V1 above.	As identified in V1 above.	As identified in V1 above.
	V4	Implement a City-wide policy on third parties to address the City's position on third party privacy program management.	As identified in V1 above.	As identified in V1 above.	As identified in V1 above.	As identified in V1 above.