OFFICE OF THE
City Auditor

Information Protection Readiness for Securing Personal Information

May 23, 2014

THE CITY OF Edmonton

The Office of the City Auditor conducted this project in accordance with the *International Standards for the Professional Practice of Internal Auditing*

Information Protection Readiness for Securing Personal Information

Table of Contents

This page intentionally left blank

Information Protection Readiness for Securing Personal Information

1. Introduction

As part of its 2013 Annual Work Plan, the Office of the City Auditor (OCA) included a review of the City's readiness to secure personal information that it controls or is in its custody. The overall objective of this audit was to evaluate the methods used by the City to secure personal information.

2. Background

FOIP Legislation
The requirement for a public body to secure personal information is prescribed in section 38 of the current version of the FOIP (Freedom of Information and Protection of Privacy) Act. Specifically, it requires that public bodies "protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction." The corresponding *FOIP Guidelines and Practices* (FOIP Guidelines)[1] further detail what are reasonable security arrangements and include the following:

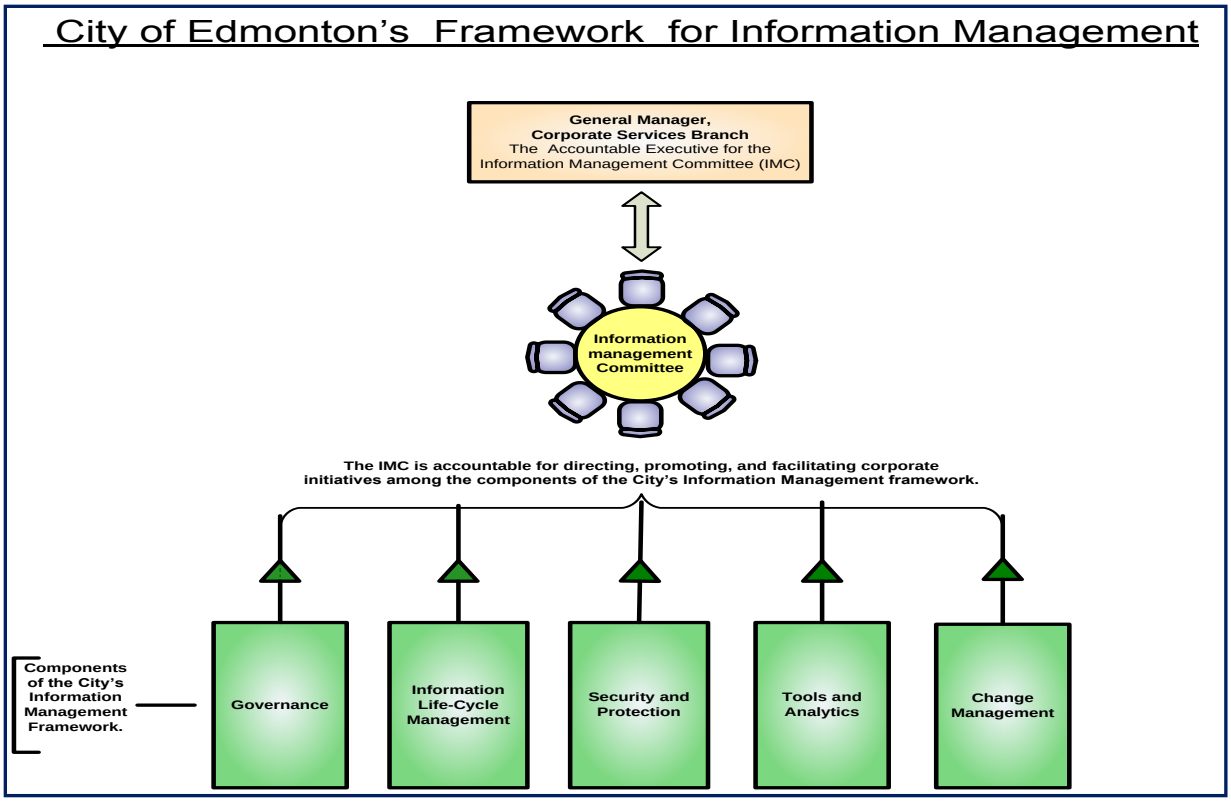
a. Information security policies (i.e., governing documents)
b. Risk assessments and risk management of personal information
c. Processes to identify and classify sensitive information, and
d. A combination of security procedures that cover administrative, physical and technological safeguards

Information Management at the City of Edmonton
The protection and security of personal information forms a key component of the City's overall goal to manage City information in a disciplined, coordinated and secure manner. The City's Information Management Committee (IMC) is the management group that has been established to support this goal, specifically through the direction, promotion, and facilitation of corporate initiatives among the components of the City's information management framework.

In terms of authority and accountability, the General Manager of Corporate Services is the chair of the IMC. However, as per the Employee Code of Conduct handbook, every City employee is ultimately responsible for managing corporate information assets in a secure manner. The City's information management framework is illustrated in Figure 1 on the following page.

[1] The Province of Alberta's *FOIP Guidelines and Practices:* Chapter 7, s.7.5 and Chapter 9, s.9.5

Figure 1:



Securing personal information in the City

Within the City of Edmonton, the personal information of 630,328 taxpayers[2] and 9,204 employees[3] is retained to conduct daily activities. Bylaws, directives, and procedures (governing documents) are used to administer the protection of this personal information as well as other forms of personal information (see Appendix 1). Additionally, technological safeguards such as passwords, encryption, virus and network monitoring technologies are combined with physical safeguards such as access cards, security cameras, and restricted zones to support the City's effort to secure personal as well as general City information.

3. Objectives, Scope, & Methodology

3.1 Audit Objectives and Criteria

The objective of the audit was to determine if the City is employing reasonable security arrangements (methods) to protect the personal information it controls and is in its

[2] The figure of 630,328 taxpayers represents the total amount of property owners paying property taxes in the City of Edmonton as at November 1, 2013.

[3] The figure of 9,204 employees represents the total number of employees employed by the City of Edmonton as at November 1, 2013. It does not include employees of the Edmonton Police Service or the Edmonton Public Library as these organizations are classified as separate entities.

custody in accordance with section 38 of the current version of the Province of Alberta's FOIP Act (FOIP Act).

We evaluated the objective against the following criteria:

1. Authority and responsibility to secure and protect personal information has been established and delegated.
2. An assessment identifying sensitive information, valuable assets, and information systems has been performed.
3. A threat and risk assessment assessing the risks to information and information systems and identifying what information is likely to require additional safeguards has been performed.
4. Administrative safeguards to secure personal information exist and are being implemented.
5. Physical safeguards to secure personal information exist and are being implemented.
6. Technological safeguards to secure personal information exist and are being implemented.

3.2 Scope and Methodology

The scope of the audit focused on reviewing the methods used by the City to secure personal information it controls and is in its custody in accordance with the FOIP Act. The methods were evaluated for reasonableness using corresponding guidance provided in the FOIP Guidelines.[4]

Other than evaluating the reasonability of the City's compliance to section 38, the audit did not evaluate the City's information management program to any other section in the FOIP Act nor were the components of the City's information management framework reviewed. Further, the City's information management processes, such as the collection, storage, and destruction of information, were not evaluated in this audit.

The audit's methodology included a risk planning process that was used to identify key risks with the City's methods to protect personal information. Several tests were used to evaluate the audit objective including a policy review of relevant governing documents, tests of controls, interviews with management and key stakeholders, and reviews of the City's *FOIP Annual Reports*.

4. Observations and Recommendations

4.1 Authority and responsibility for the protection of personal information

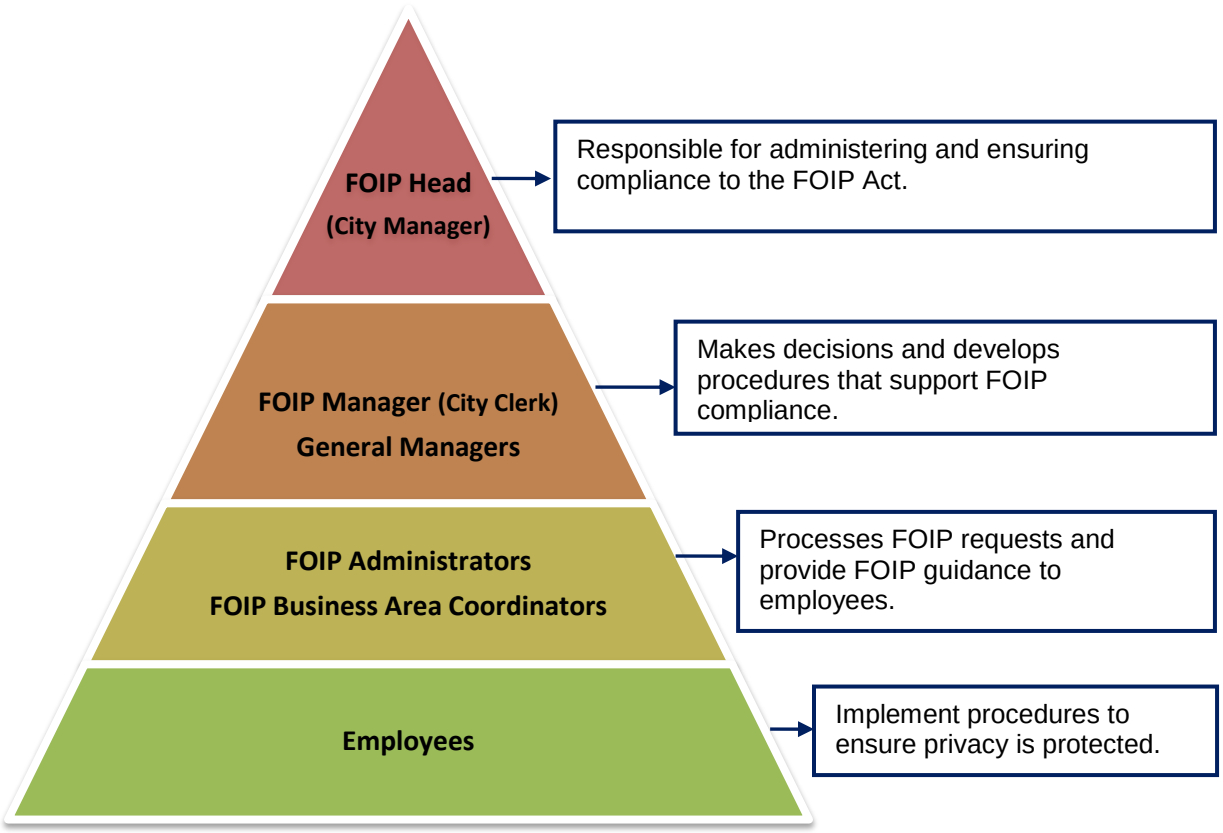
To ensure that personal information is properly secured in accordance with section 38 of the FOIP Act, a public body must first ensure that the appropriate level of authority and responsibility for FOIP compliance, in general, has been established.

[4] Province of Alberta's *FOIP Guidelines and Practices* Chapter 7, s.7.5 and Chapter 9, s.9.5

Administration of the FOIP Act

The City's FOIP Bylaw (12001) appropriately delegates the authority and responsibility for the FOIP Act to the City Manager (as FOIP Head). The City Manager is the most senior employee of the City's Administration and is appointed by City Council. This means that the City Manager is ultimately responsible and accountable for ensuring that reasonable security arrangements are made to protect personal information in accordance with the FOIP Act. The City's FOIP Delegation Order further delegates this responsibility to the City's General Managers, FOIP Manager, FOIP Coordinators, and Information Access Coordinators. Finally, City employees are expected to follow related procedures and controls and are ultimately responsible for securing personal information. Figure 2 below illustrates the general administration of FOIP in the City.

Figure 2: Administration of FOIP in the City of Edmonton



Clarification of Section 38 in the FOIP Delegation Order

As the FOIP Head, the City Manager has issued a Delegation Order which delegates authority to General Managers, the FOIP Manager, FOIP Coordinators, and other City employees managing FOIP functions. The Delegation Order assigns accountability and responsibility for each section of the FOIP Act, by determining which employees will "**ensure**" compliance and which employees will "**assure**" that compliance occurs.

With regards to section 38 however, the OCA determined that the terms "assure" and "ensure" do not make a clear enough distinction between the employees that are

accountable for giving direction and the employees that are responsible for implementing direction to protect the security of personal information. The Delegation Order should be revised to clearly convey the accountability and responsibility for section 38.

Recommendation 1: FOIP Delegation Order

That the General Manager of Corporate Services prepare amendments to the FOIP Delegation Order for the FOIP Head's approval, that clarify accountability and responsibility for section 38 delegations.

Management Response and Action Plan

Accepted.

Action Plan: The FOIP Delegation Order will be amended to clearly establish which employees are accountable for powers, duties and functions under the FOIP Act, and which employees are responsible for implementing direction from those who are accountable for decision making. The amended delegation order will be put forward for the FOIP Head's approval.

Planned Implementation Date: September 30, 2014
Responsible Party: Law Branch, City Solicitor
To Close: Delegation Order approved by FOIP head (City Manager)

4.2 Assessing threats and risks to information

Assessing threats and risks to information and information systems enables an entity to identify what information is likely to require safeguards. This provides a good basis for developing adequate information security controls (controls).

Threat and risk assessments to information and information systems

Four formal methods are used by the City to conduct threat and risk assessments to major information and information systems projects (major projects):

1. The *Privacy Impact Assessment (PIA)* form is used whenever new programs, schemes and/or automated information systems are being developed. PIA's compel the user to assess the privacy risks to personal information in major projects.
2. In advance of completing a PIA, business areas can choose to complete a *Privacy Impact Evaluation form (*PIE), which is a condensed version of the PIA. Once completed, the PIE is used by the City's FOIP Office to determine if a PIA is needed.
3. The *Privacy Impact and Risk Assessment* form is used specifically by the Information Technology (IT) Branch in lieu of the PIA/PIE forms. It assesses the privacy impact of technology solutions that will have a widespread impact to City information.
4. The *Information Risk Assessment* form is also used by the IT Branch to specifically assess the information risk in major projects.

Together, these documents can be used by business areas to conduct threat and risk assessments to major projects.

The OCA obtained a listing of eight major projects that were implemented in the last five years and reviewed the formal threat and risk assessments for six of those projects. Management has indicated that they reviewed the remaining two systems and determined that these systems would not capture personal information. Therefore, no formal risk assessment was conducted for these two systems. It is good practice to document threat and risk assessments, regardless of the outcome, since it provides management with a record and documented rational for its choice in information security controls in a major project.

4.3 Formal method of classifying City information

A process to classify information should be in place to ensure that sensitive information, such as personal information, is identified and adequately secured. For example, a system could classify information according to the *level of security* required (i.e., restricted vs. unrestricted) and according to the *nature* of the information (i.e., personal vs. public).

Classifying City information

The OCA found that methods to classify the sensitivity of information do exist in the threat and risk assessment forms discussed earlier. However, these documents are only completed whenever major projects take place. Based on our review, the OCA determined that a formal process to classify the sensitivity of information in the course of day-to-day City work does not exist. Such a method would ensure that all sensitive information is properly identified and classified and on a consistent basis throughout the City.

Based on discussions with management, steps are being taken to address this gap. Management has asserted that the IMC is currently drafting an updated Information Management directive that will centralize and provide guidance on securing City information. This directive will also include a methodology to classify City information based on its nature and security requirements. When finalized, this directive should support the City's effort to ensure that personal information is properly identified, classified, and ultimately secured. (See Recommendation 2)

4.4 Administrative, Physical, and Technological Safeguards

In addition to assessing risk and classifying information, the FOIP Guidelines suggest a set of administrative, physical, and technological safeguards that will support security of personal information in a public organization.

4.4.1 Administrative safeguards

Administrative safeguards are defined as administrative actions, policies, and procedures that facilitate the management of an organization's information security program. The OCA assessed the appropriateness of the City's administrative

safeguards by comparing them to those suggested in the FOIP Guidelines. As displayed in Table 1, the City has established the administrative safeguards suggested by the FOIP Guidelines. However, we found that improvements can be made to enhance their implementation.

Table 1: Administrative Safeguards in Place at the City of Edmonton

Administrative Safeguard	City of Edmonton
1. Designating a position that has overall responsibility for information security within the public body.	In place
2. Ensuring that staff understands their responsibilities and the public body's security procedures by providing them with written procedures.	In place
3. Ensuring that staff understands their responsibilities and the public body's security procedures by instituting training programs.	In place
4. Arranging to resume operations in the case of loss of computer-based data or capabilities.	In place
5. Performing background and reference checks of officers and employees to ensure that he/she is a suitable person to have access to sensitive information, information systems and the facilities where they are located.	In place
6. Implementing the "need-to-know" principle where access to particular information systems can be limited to certain officers and employees who have a need for such access because it is necessary to perform their duties.	In place
7. Conducting process audits and periodically reviewing access logs, etc.	In place
8. Establishing sanctions for breaches of information security and a process for reporting and investigating breaches.	In place

Comprehensive information security governing documents

Through the OCA's review of the policies, we determined that procedures to secure personal information are spread throughout a variety of bylaws, administrative directives, administrative procedures and guidelines (see Appendix 1). Each of these governing documents has a different purpose and objective and therefore does not singularly address nor comprehensively discuss the security of personal information.

This may create a challenge for employees that must piece the information in these governing documents together in such a way that their responsibility to secure personal information is made clear, understood, and properly implemented. Without such clarity, there is a risk a poor understanding of the governing documents may lead to privacy breaches. A governing document(s) that focuses on information security and comprehensively discusses the security of personal information would mitigate this risk.

As discussed in report section 4.3, as part of the effort to develop the Information Management directive, the IMC is currently reviewing the City's governing documents that concern information management and is identifying areas of improvement. As indicated by management, the intent of the directive is to facilitate employees' understanding of their responsibilities to secure personal information.

Recommendation 2: Comprehensive Governing Document

That the General Manager of Corporate Services develops and finalizes a focused and comprehensive information security governing document(s). The governing document(s) should include a methodology to classify the sensitivity of information and provide guidance on administrative, physical, and technological safeguards which support information security.

Management Response and Action Plan

Accepted.

Action Plan: Corporate Services will develop governing documents to define guidelines and standards related to information security for approval by the City's Corporate Leadership Team.

Planned Implementation Date: April 30, 2015
Responsible Party: Information Technology, Branch Manager
To Close: Governing docs approved by CLT

Ongoing FOIP and information security training

When initially hired, City employees are required to take mandatory Employee Code of Conduct training which includes information and asset security training. Additionally, the *FOIP in the City* course is available to all employees and provides an overview of the FOIP Act and the City's FOIP program.

The City also has FOIP Coordinators, who provide advice on records and FOIP matters and also handle FOIP requests for their respective departments. In addition to the *FOIP in the City* training course, FOIP coordinators must take advanced training for preparing records for public disclosure. The City's FOIP office also provides training across the Corporation upon request which is tailored to the issues normally encountered by the area receiving the training. Combined together, these components are designed to ensure that City employees are aware of their responsibilities to secure the privacy of City information.

A review by the OCA of the City's *FOIP Annual Reports* however suggests that ongoing training should be provided to employees who regularly handle personal information. This will ensure that such employees are continuously equipped with the most current knowledge to secure personal information. (See Recommendation 3)

4.4.2 Physical safeguards

Physical safeguards are physical measures designed to protect an entity's information systems as well as buildings and equipment from unauthorized intrusion and from natural and environmental hazards. The OCA assessed the appropriateness of the City's physical safeguards by comparing them to those suggested in the FOIP Guidelines. As displayed in Table 2, the City has implemented the physical safeguards suggested by the FOIP Guidelines. However, an improvement can be made to enhance their implementation.

Table 2: Physical Safeguards in Place at the City of Edmonton

Physical Safeguard	City of Edmonton
1. Periodic reviews of physical security features, such as alarms, fences, and codes for programmable keypad door locks.	In Place
2. Use of physical barriers, security zones, access and authorization mechanisms, and locked containers to restrict access.	In Place
3. Specifying adequate fire and fire safety procedures.	In Place
4. Designating off-site storage facilities with a similar level of physical and environmental security.	In Place

Ongoing training of physical security procedures

Throughout the year**,** Corporate Security conducts proactive testing to ensure that City facilities contain adequate security features and are physically secure. These tests include scheduled security audits and random security penetration tests (proactive tests).

Corporate Security has indicated that in the past year over 85% of the resulting security recommendations have been accepted. Corporate Security has also indicated that there have been no recorded incidents where the protection of personal information has been compromised as a result of a physical security breach. Corporate Security further noted that human error alarms have also decreased, which they believe is due to the positive effect that training is having on employee behavior.

The OCA observed that security incidents in City facilities have been trending downward. However, results from a sample of proactive tests reviewed by the OCA suggest the need for employees to receive ongoing training about the City's physical safeguards. (See Recommendation 3)

4.4.3 Technological safeguards

Technological safeguards represent the final layer of safeguards suggested by the FOIP Guidelines to secure personal information. Technological safeguards are controls built within electronic information systems and are designed to secure the confidentiality and integrity of information held therein. As displayed in Table 3, the City has established the technological safeguards suggested by the FOIP Guidelines. However, an improvement can be made to enhance their implementation.

Table 3: Technological Safeguards in Place at the City of Edmonton

Technological Safeguard	City of Edmonton
1. Use of software, hardware or operating system access controls such as passwords, termination on inactivity, and clearance of display screens, transaction logs and error logs.	In place
2. Use of secure communications and encryption, especially for mobile devices such as laptops.	In place
3. Use of virus protection for new and existing computer equipment.	In place
4. Use of security controls for remote access to information systems.	In place

Downloading City information onto personal devices

For its own electronic mobile devices, the City uses secure communications and encryption technologies to ensure that City information retained on these devices is adequately protected. City-owned mobile devices also include anti-virus software which safeguards the integrity of City information and remote-find-and-wipe software which deletes City information should a user lose a City-owned mobile device.

City employees can also use their own smartphones, tablets, and computers (personal devices) to conduct work with City information that is accessible through their corporate emails. While employees cannot access the City's network using their personal devices, currently employees can download City information (i.e., as attachments) from their corporate emails onto their personal devices. Since the personal devices of City employees are not subject to the same controls as City-owned devices, City information retained on personal devices may be compromised and/or subject to unauthorized use.

According to the City's Code of Conduct, employees must not download "personally identifying information, confidential third party or City information to [their] personal phone or device without the permission [from] their supervisor." Despite this policy however, management has indicated that they are aware that employees may be downloading data onto their personal devices and are also aware of the risk it presents to City information. Through the implementation of the Information Management directive (see report sections 4.2 and 4.3) and FOIP training programs, management intends to reduce and ultimately eliminate the occurrence. To safeguard the security of

City information in electronic form, management should ensure that employees are aware of their obligation to avoid downloading City information.

Recommendation 3 - Implement ongoing FOIP and information security training

That the General Manager of Corporate Services, with the approval of the City's Corporate Leadership Team, develop and implement a strategy to identify and provide ongoing FOIP and information security training to employees who regularly handle personal information.

Management Response and Action Plan

Accepted.

Action Plan: Administration will develop targeted training strategy for physical security, technical security and FOIP awareness for CLT approval. Corporate Services will work with client areas to provide the appropriate training for employees who regularly handle personal information.

Planned Implementation Date: September 30, 2015
Responsible Party: Corporate Services, General Manager
To Close: Training strategy approved by CLT

5. Conclusion

Section 38 of the existing version of the Province's Alberta's FOIP Act requires that a public body protect personal information by making reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure and destruction. The objective of the audit was to determine if the City was employing reasonable security arrangements to secure the personal information it controls and is in its custody in accordance with section 38 of the FOIP Act.

The complementing Guidelines[5] to the FOIP Act ultimately define *making reasonable security arrangements* as "approving and implementing an information security policy (i.e., governing document)." We found that the City is in the process of developing an information management governing document (i.e., directive) that will include comprehensive and focused guidance on information security and the security of personal information for City employees.

We also found that the City established appropriate authority for information security and the existence of administrative, physical, and technological safeguards suggested by the FOIP Guidelines.

However, to improve the implementation of the City's safeguards and ultimately enhance its ability to secure personal information, we recommend the following actions:

1. Revision and clarification of the FOIP Delegation Order in relation to section 38. Clarity of the Delegation Order will support a stronger framework for the protection of personal information in the City.

2. Implementation of a strategy that will identify and provide ongoing FOIP and information security training to employees who regularly handle personal information. By providing relevant employees with ongoing training, the City will be able to ensure the security of critical information.

3. Implementation of a focused and comprehensive information security governing document(s). The governing document(s) should include a methodology to classify the sensitivity of information and guidance on administrative, physical, and technological safeguards which support information security.

Together, these improvements will support the City's effort to ensure that reasonable security arrangements are in place to protect personal information.

[5] The Province of Alberta's *FOIP Guidelines and Practices:* Chapter 7, s.7.5 and Chapter 9, s.9.5

Appendix 1: Relevant Governing Documents

Table 4 summarizes governing documents at the City of Edmonton that concern the protection of personal information.

Table 4: Relevant Governing Documents at the City

Governing Document	Responsible Department	Purpose
FOIP Bylaw 12001	Office of the City Manager	Establishes the administrative structure for the administration of FOIP in the City.
Privacy Directive (A1433A) Privacy Procedure (A1433A) and Privacy Code (A1433A)	Office of the City Manager	Establishes the commitment and prescribes procedures to protect all recorded personal information retained by the City.
Corporate Records and Information Management Directive (A1410C) Corporate Records and Information Management Procedure (A1410C)	Office of the City Manager	Establishes and prescribes a standard records and information management framework that will reasonably ensure the proper capture, protection, use, and preservation of City records as evidence of the City of Edmonton functions, activities, and business transactions.
Acceptable Use of Communication Technology Directive (A14129C) Acceptable Use of Communication Technology Procedure (A14129C)	Corporate Services	Establishes and provides standards and guidelines for employees and other users when transmitting, storing, and accessing communication technology in the City.
Protection of Mobile Sensitive Data Directive Protection of Mobile Sensitive Data Procedure(A1444)	Office of the City Manager	Establishes and prescribes procedures that safeguard data stored on mobile data storage devices (i.e., USB's, laptops, tablets, etc.,)
Code of Conduct	Corporate Services	Prescribes several methods that employees must implement to safeguard personal information that is used during the course of daily City activities.