OFFICE OF THE
City Auditor

Audit of Privacy Controls for Laptops & Tablets

November 3, 2009

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*

Audit of Privacy Controls for Laptops & Tablets

Table of Contents

Audit of Privacy Controls for Laptops & Tablets

Summary for City Council

The City of Edmonton uses laptop and tablet computers (mobile devices) to carry out its routine business. Some of these mobile devices contain personal information (recorded information about an identifiable individual). At the end of 2008, the City had 859 laptop and 345 tablet computers in use. Organizations are required to ensure that the personal information they collect and store is continually protected as required by privacy legislation.

The Office of the City Auditor conducted an audit of privacy controls to provide assurance that appropriate safeguards are in place to protect personal information residing on mobile devices. A full report outlining the detailed results of our audit follows. The purpose of this summary is to highlight areas requiring improvement by Administration and any direction that Council may need to provide to Administration in order to fulfill its governance and oversight role.

A privacy breach occurs when personal information is collected, used or disclosed in ways that are contrary to privacy legislation. An example is when a mobile device containing personal information is lost or stolen. Over the last four-year period, the City estimates that it has lost one mobile device per month (12 mobile devices annually). We found that with one exception in the last four years, the City did not specifically determine whether the lost or stolen mobile devices contained any personal information.

The Office of the Information and Privacy Commissioner of Alberta recommends three layers of security and safeguards (physical controls, technical controls, and administrative controls) to protect personal information on mobile devices. With a layered security approach, each layer offers an incremental level of protection to the electronic data if a device with personal information on it is stolen or is reported missing.

Our overall assessment of internal controls over personal information on the City's mobile devices is that:

- It has implemented reasonable *physical controls* to protect personal information on mobile devices. We have suggested some opportunities for improvement to enhance these controls.
- The City has not implemented reasonable *technical* and *administrative controls* to protect personal information on mobile devices.

The root cause of the gaps between a strong internal control environment and the City's actual practices is the lack of clarity in roles, responsibilities, accountabilities and authority for managing personal information on mobile devices. We have recommended that Corporate Services develop an implementation plan to resolve the identified issues. The Administration intends to complete its plan by June 2010. Although our recommendation focuses on developing a plan, it is essential that all of the identified control weaknesses be resolved promptly.

We also found that only approximately 50% of the stolen or missing devices are investigated. The corporate investigation process needs to be strengthened in several areas. We have recommended that Corporate Services develop and formalize a corporate investigation process to be followed for all laptop and tablet computers reported stolen or missing. The Administration plans to complete this by June 2010.

In our opinion, it is essential for Corporate Services to give priority to implementing our recommendations. This will ensure that appropriate safeguards are in place to protect personal information on laptop and tablet computers. Although our recommendations are directed to laptop and tablet computers, Corporate Services needs to ensure that all mobile devices (not just laptop and tablet computers) are safeguarded and included in its implementation strategy.

Audit of Privacy Controls for Laptops & Tablets

1. Introduction

The Office of the City Auditor's (OCA) work plan included an audit of internal controls relating to personal information that is transferred from the City of Edmonton corporate network to mobile devices (laptop and tablet computers). When an organization collects and stores personal information, its primary focus must be to ensure that an individual's privacy is continually protected.

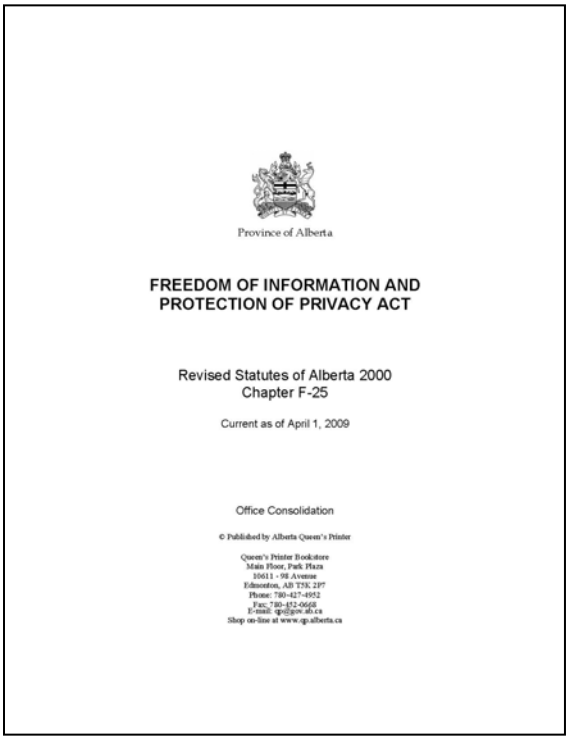
Our overall objective for this audit was to provide assurance that appropriate safeguards are in place to protect personal information on laptop and tablet computers (herein referred to as mobile devices).

2. Background

2.1. Privacy Environment

Personal Information

Alberta's Freedom of Information and Protection of Privacy (FOIP) Act[1] provides individuals the right to request access to information in the custody and control of public bodies. It also provides a framework within which public bodies (City of Edmonton is defined as a public body) must[2] conduct collection, use, and disclosure of personal information.


Province of Alberta

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Revised Statutes of Alberta 2000
Chapter F-25

Current as of April 1, 2009

Office Consolidation

Queen's Printer Bookstore
Main Floor, Park Plaza
10611 - 98 Avenue
Edmonton, AB T5K 2P7
Phone: 780-427-4952
Fax: 780-452-0668
E-mail: qp@gov.ab.ca
Shop on-line at www.qp.alberta.ca

Personal Information is defined formally in the FOIP Act. It means recorded information about an identifiable individual, including (but not limited to) the individual's name, home or business address or home or business telephone number, the individual's race, national or ethnic origin, religious or political beliefs or associations, the individual's age, sex, marital or family status, information about the individual's health, education, financial, employment or criminal history, opinions of others about the individual, etc. Appendix 1

[1] **Province of Alberta, Freedom of Information and Protection of Privacy Act**, Revised Statutes of Alberta 2000, Chapter F-25, and Current as of April 1, 2009.

[2] The word "must" signifies mandatory requirements in contrast to other sections of FOIP where the word "may" is used.

provides the complete definition of "Personal Information" as outlined in Section 1(n)(i - ix) of the FOIP Act.

Privacy Breach

A privacy breach occurs when personal information is collected, used or disclosed in ways that are contrary to the provisions of FOIP or other privacy Legislation (e.g., PIPA – Personal Information Protection Act, PIPEDA – Personal Information Protection and Electronic Documents Act). A common breach of personal privacy is the unauthorized use or disclosure of personal information. For example, if a mobile device with personal information stored on it is lost or stolen, a privacy breach under FOIP has occurred. It is the Privacy Commissioner of Alberta's position that individuals should be notified of privacy breaches where there is a potential for harm resulting from the unauthorized disclosure of personal information. The Commissioner has also indicated that significant resources are expended by organizations to notify affected individuals following a privacy breach. Consequently, implementing a strong control environment can reduce such expenditures.

Office of the Information and Privacy Commissioner of Alberta

FOIP Act Section 53 (General Powers of Commissioner) states:

> In addition to the Commissioner's powers and duties under Part 5 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may conduct investigations to ensure compliance with any provisions of this Act or compliance with rules relating to the destruction of records.

In conducting its investigations into privacy breaches involving mobile devices, the Commissioner has determined certain requirements associated with providing reasonable security precautions with due regard to an assessment of:

- Foreseeability of security risk and likelihood of damage;
- Seriousness of the harm;
- Cost of preventative measures; and
- Relevant standards of practice.

The Commissioner's office has stated, "Frequent incidents of laptop theft from employees, often despite corporate policies, are well known and publicized, making the risk real and foreseeable." They recommend three layers of security and safeguards in order for public bodies to discharge their obligations to protect personal information on mobile devices in their custody or control:

1. Physical security (locked cabinets, cable locks, motion sensor alarms, keeping devices in sight, etc.),

2. Technical protection measures (encryption, remote access, call home and remote "kill switch" commands, etc.), and
3. Administrative measures (behavioural rules and their enforcement, such as policies to restrict the amount, type, and time data is kept, "need to know rules," process audits, random laptop audits, etc.).

As illustrated in the Report of the Auditor General of Alberta (Protecting Information Assets - October 2008) security is layered like an onion. Layered protection requires significantly more effort and skill to penetrate, thereby reducing the risk of unauthorized access.[3]

FOIP Act Section 38 (Protection of Personal Information) states that, "The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction of personal information."

Recently, an individual (privacy breach incident not related to the City of Edmonton) was fined $10,000 for unauthorized access to personal health information. In his news release, the Privacy Commissioner emphasized that "…surfing records for personal purposes will not be tolerated and individuals will be prosecuted." Furthermore, the Commissioner indicated that as organizations "…move increasingly to electronic…records, the security of…[personal] information remains paramount."[4]

Also, the Privacy Commissioner of Canada has found that although an organization may have policies in place regarding device security, the organization is still accountable when employees fail to comply with those policies.

City of Edmonton's Formal Commitment to Privacy

Administrative Directive A1433A, *Privacy* (June 11, 2004) contains the following purpose statements:

> To ensure the City of Edmonton is in compliance with the privacy provisions of the *Freedom of Information and Protection of Privacy Act*

[3] **Onion Skin Approach:** "When designed properly, multilayer network security looks like an onion. You need to keep peeling layers off to get to the critical core. One layer of security inside another protects valuable assets. If security systems aren't properly designed, you can bypass the security layers and cut directly to the center." (Report of the Auditor General of Alberta Protecting Information Assets–October 2008.)

[4] **Office of the Information and Privacy Commissioner of Alberta**, News Release: Commissioner Responds to Health Information Court Case (April 17, 2009) "A medical office clerk from Calgary pleaded guilty to charges of improperly accessing another person's medical information, in contravention of the *Health Information Act* (HIA). The individual appeared in Calgary Court Friday and was fined $10,000. This is the first time that charges have been laid under the HIA." This outcome resulted from a complaint to the Privacy Commissioner several years earlier. Upon completion of the investigation into the original complaint, the Commissioner referred the matter to the Regulatory Prosecution Office of Alberta Justice (News Release, November 23, 2006).

and to establish commitment to the protection of all recorded personal information about an identifiable individual.

To ensure that whenever a system involving personal information is being developed or substantially changed, the City of Edmonton undertakes a Privacy Impact Assessment to analyse potential impacts on privacy and to ensure the City takes measures to make the system compliant with this directive.

There are many other administrative directives that provide additional guidance and direction when dealing with personal information on mobile devices (following section).

2.2. Directing Framework

The City has a framework of bylaws, and administrative directives (including associated procedures and guidelines) that directs, in varying degrees, the approach to dealing with personal information. The full listing is provided below:

Bylaws

- Bylaw 12100: *Freedom of Information and Protection of Privacy Bylaw* (September 14, 1999)
- Bylaw 12101: *Corporate Records and Information Management Bylaw* (October 1, 1999)

Administrative Directives

- Administrative Directive A1100C: *Employee Code of Conduct* (June 27, 2002)
- Administrative Directive A1433A: *Privacy* (June 11, 2004)
- Administrative Directive A1429B: *Acceptable Use of Communication Technology* (October 25, 2005)
- Administrative Directive A1444: *Protection of Mobile Sensitive Data* (May 24, 2007)
- Administrative Directive A1445: *Privacy Breach* (May 24, 2007)
- Administrative Directive A1410C: *Corporate Records And Information Management Program* (March 13, 2008)

Dated Administrative Directives

- Administrative Directive A1409A: *Computer Systems* (March 23, 1989)
- Administrative Directive A1414A: *Computer Access Security* (October 18, 1989)

These measures apply to all employees reporting to the City Manager and employees in the Office of the City Auditor. The specific directing measures do not apply to elected officials or their assistants. However, there is guidance on the application of FOIP for records of elected officials.[5]

[5] **Records of Elected and Appointed Officials of Local Public Bodies**, FOIP Bulletin, Number 6, Revised March 2009, Access and Privacy Services Alberta

3. Objective

The objective of this audit was to provide assurance that appropriate safeguards (consistent with best practices) are in place to protect personal information on the City's mobile devices (i.e., laptop and tablet computers).

4. Scope and Methodology

4.1. Audit Scope

The City's definition of Mobile Data Storage (Administrative Directive A1444: *Protection of Mobile Sensitive Data*) is:

> This refers to any means of storing electronic information that is small and relatively portable. Examples include (but are not limited to) laptop computers, tablet computers, personal digital assistants (PDAs), Blackberrys, universal serial bus (USB) flash memory sticks, portable disk drives, diskettes, data tapes, and CDs & DVDs (various types). NOTE: Mobile Storage Data might be City assets, but there could be personally owned Mobile Data Storage which is being used to store City information.

For this audit, we limited our audit scope to two specific types of mobile computing devices: laptop and tablet computers. Laptops are portable general purpose personal computers. Tablets are a subset of Laptops, which have a touch-sensitive display screen (can accept input from not only a keyboard but also hand-written notes). These mobile devices are at high risk of being stolen and any personal information that is stored on them presents the risk of a privacy breach.

4.2. Audit Methodology

Safeguarding Personal Information on Mobile Devices

The Office of the Information and Privacy Commissioner of Alberta recommends a layered approach to protect personal information, including physical, technical, and administrative controls. This ensures that reasonable protection against unauthorized access is provided if the mobile device is stolen or reported missing.

The Privacy Commissioner of Alberta has conducted several investigations[6] and reported extensively on the specific safeguards that must be in place to protect personal information on laptop and tablet computers. The results of these investigations formed our basis for identifying the specific elements of each type of recommended control. Inadequate maintenance of recommended safeguards to protect personal information on mobile devices poses two risks for the City (in the event that an actual complaint was made to the Commissioner's Office):

- The Commissioner's office could draw a conclusion that the City contravened the FOIP Act, and
- The Commissioner's office could outline steps to the City that must be taken to protect personal information stored on a mobile device in order to meet requirements of the FOIP Act.

We adopted these specific elements as our detailed audit criteria. By being proactive and ensuring that the elements in each of the three controls are in place, there is reasonable assurance that personal information on mobile devices is protected.

We compared the City's framework and actual practices against the audit criteria in order to assess the effectiveness of the City's safeguards. We also conducted a walk-about through a sample of office floors in Chancery Hall and Century Place to observe the general level of physical security over mobile devices.

The Commissioner's required controls are best understood as "reasonable safeguards for protecting personal information" on laptops and tablets. "Reasonable" is defined as "what a reasonable person would consider appropriate in the circumstances."[7] It is important to point out that "reasonable" does not mean "absolute." Personal information security breaches may still occur, even when reasonable safeguards have been

---

[6] **Office of the Information and Privacy Commissioner of Alberta: "**Report on an Investigation into the Security of Personal Information", September 26, 2006, MD Management Ltd., Investigation Report P2006-IR-005.

Office of the Information and Privacy Commissioner of Alberta: "Report of an Investigation Concerning a Stolen Laptop Computer", December 5, 2006, Calgary Health Region, Investigation Report H2006-IR-002 (Investigation H1441).

Office of the Information and Privacy Commissioner of Alberta: "Investigation Report Concerning Stolen Laptops Containing Health Information", November 5, 2007, Capital Health, Investigation Report H2007-IR-02 (Investigations H1652, H1726, H1733, H1742 & H1746).

Office of the Information and Privacy Commissioner of Alberta: "Investigation Report Concerning a Stolen Laptop Containing Health Information", October 21, 2008, East Central Health, Investigation Report H2008-IR-003 (Investigations H2200).

Office of the Information and Privacy Commissioner of Alberta: "News Release – Level of Security on Stolen Laptops Simply Not Acceptable, say Commissioner" June 24, 2009 (two laptops containing health information stolen from Alberta Health Services were not encrypted).

[7] **Office of the Information Privacy Commissioner of Alberta:** Personal Information Protection Act (PIPA), PIPA Advisory #8, Implementing Reasonable Standards (This definition is commonly used by Privacy Commissioners across Canada).

implemented. Instead, reasonable standards require organizations to take into account all relevant circumstances in determining what safeguards to implement.

Review of Corporate Response to a Report of a Lost or Stolen Mobile Device
We assessed the current controls, processes and practices once a mobile device is reported as lost or stolen. We interviewed key participants involved in the various corporate activities (Corporate Security, Risk Management, IT Security, and FOIP staff). This review focused on the investigative processes, and not on the specific loss or theft incidents.

We also observed a demonstration of a security product the City uses on mobile devices. This product has the functional capability to:

- Track a stolen mobile device, and/or
- Wipe clean the entire contents of the device's storage.

Our goal was to assess the extent to which the City is exercising due diligence when mobile devices are reported as either missing or stolen.

5. Summary of Results

5.1. Data Analysis

Inventory of Mobile Devices
The City was leasing 1,204 laptop and tablet computers as of December 2008. Of this total, there were 859 laptops (71%) and 345 tablet computers (29%).

Trend Data for Missing and Stolen Devices and Materiality of the Loss
We conducted a trend analysis of mobile devices stolen or reported missing for the period of 2005 to 2008. Over this period, the City has recorded an average loss of one mobile device per month (12 annually). The actual lease-buyback charges incurred for these stolen or missing devices over the reported period ranged from $480 to $5,573, with an average of $1,852 per device. If the device is not recovered, the City is now eligible to receive equivalent-to-insurance of $600 to $1,000 per device (some conditions apply).

However, the replacement cost of a mobile device is often the least expensive item. There are many other considerations (soft costs) such as: employee downtime, cost to repair damage to devices if recovered, investigation and recovery costs, potential identity theft, loss of corporate reputation, potential exposure of corporate data to outsiders, investigation of a potential privacy breach, costs associated with notification, etc. The City of Edmonton, does not track these soft costs.

Loss of Personal Information
Historically, the investigation protocol was focused on the physical device itself, rather than the information that was stored on the device. Of all the investigation files we reviewed, only one case file contained evidence that the investigation determined whether or not personal information was on the device. In this instance, the investigator concluded that resumes had been stored on the mobile device and initiated a privacy breach investigation. The Administration does not have defined/formal processes in place to allow investigators to determine whether or not personal information was stored on the mobile devices reported stolen or missing. In the absence of such processes, no estimate can be made of both the incidence and significance of privacy breaches that could have taken place with a lost or stolen mobile device.

5.2. Three Questions Raised

We have grouped our observations and responses to address three basic questions:

1. Are there reasonable *physical controls* for protecting personal information on mobile devices? (Section 5.2.1)
2. Are there reasonable *technical controls* for protecting personal information on mobile devices? (Section 5.2.2)
3. Are there reasonable *administrative controls* for protecting personal information on mobile devices? (Section 5.2.3)

5.2.1. Are there reasonable *physical controls* for protecting personal information on mobile devices?

Ensuring the physical security of a mobile device may appear to be common sense. However, the importance of taking basic steps to maintain physical security cannot be understated. The following table summarizes our assessment of the City's physical controls against the Office of the Information and Privacy Commissioner's prescribed standards. It is followed by a discussion of our observations and analysis.

Compliance to Prescribed Office of the Information and Privacy Commissioner of Alberta Standards for Physical Controls

Description Of The Required Physical Controls	✓ Criteria Met OR ✗ Criteria Not Met	
	Yes	No
Formal corporate direction which states that laptops/tablets must always be safeguarded from theft.	✓	
Formal corporate direction which states that laptops/tablets must never be left unattended when out of the office (e.g. in a vehicle or hotel room).	✓	
Formal corporate direction which states that laptops/tablets must be locked in secure cabinets at home, or in a non-secure work area (even if the laptop/tablet can be secured to the workstation/desk).	✓	
Formal corporate direction which states that laptops/tablets must be carried on the airplane when traveling.	✓	
Formal corporate direction which states that when traveling: • Personal information must not be kept on a laptop/tablet unless required for work purposes during the trip, and • Eye contact must be maintained of a laptop/tablet at all times, or put it in a place where you can feel if someone grabs it.	✓	
Formal corporate direction to explicitly require that a locking cable is required to secure laptop/tablet to a desk or table (on or off City premises).	✓	

Our overall assessment of physical controls is that the City generally meets the requirements for formal corporate direction regarding physical protection of mobile devices. Opportunities for improvements to ensure full compliance can be made in the following areas:

- Consider updating, consolidating, and promoting the current number of administrative directives and procedures to something that is more manageable and friendlier towards users of mobile devices.
- Administrative Directives A1444, *Protection of Mobile Sensitive Data* (May 24, 2009) has a mandatory guideline that states: “Never store any Sensitive Data on types of Mobile Storage (especially laptop and tablet computers) which are highly targeted for theft.” This requirement does not have a technological solution, but depends on employees’ compliance.
- All users of mobile devices need to be provided a locking cable and be required to use them consistently. In our walkabout survey of several floors in two office towers, we observed that 78.5% of mobile devices were not physically secured. Although the consistent use of a cable may not physically deter a theft from occurring, its usage is consistent within the concept of a layer approach to mobile device security. No one layer provides the overall security requirement; but when all layers are in place, it makes it more difficult to access the personal information.

In our opinion, the City has established reasonable corporate directives detailing *physical controls* to protect personal information on mobile devices. We identified opportunities to strengthen this set of internal controls to proactively ensure that the City meets both the spirit and intent of the Privacy Commissioner’s requirements.

5.2.2. Are there reasonable *technical controls* for protecting personal information on mobile devices?

Electronic environments introduce a number of security risks that technical controls can help to eliminate or mitigate. The following table summarizes our assessment of the City's technical controls against the prescribed Office of the Information and Privacy Commissioner's standards. A discussion of our observations and analysis follows.

Compliance to Prescribed Office of the Information and Privacy Commissioner of Alberta Standards for Technical Controls

Description Of The Required Technical Controls	✓ Criteria Met OR ✗ Criteria Not Met	
	Yes	No
Formal corporate direction which states that files on laptops/tablets which contain personal information must be encrypted (encryption capability cannot be disabled by the user).		✗
Formal corporate direction which states that laptops/tablets must have strong log-on password standard (log-on password cannot be disabled by the user).	✓	
Formal corporate direction which states that laptops/tablets must have screen saver password protection (screen saver protection cannot be disabled by the user).		✗
To strengthen security laptops/tablets should have the capability to: • "Phone home" or "IP tracking" software which allows the stolen device to call home in the event that it is connected to the internet, • "Kill switch" software which allows the stolen device to self destruct, and • Remote access ensuring that, once the user was logged on to the network, the user would have access to files stored on it. As a result it would not always be necessary to maintain files on the laptop/tablet since they could be accessed remotely with a high speed connection (e.g., Virtual Private Network).	✓ ✓	✗

A brief discussion of the identified control issues is presented below:

Encryption: Key observations relating to this technical control include:

- The Office of the Information and Privacy Commissioner of Alberta requires that encryption be in place when storing personal information on all mobile devices. As discussed in Section 5.3, the City has limited knowledge or awareness of personal information that may be on mobile devices.
- Administrative Directive A1444, *Protection of Mobile Sensitive Data* (May 24, 2007) includes a mandatory requirement that all mobile sensitive data use an encryption solution. Progress in implementing a solution on an enterprise-wide basis is being made, with a completion date currently scheduled for Fall 2009.

- We have estimated that at least 11% of the current inventory of mobile devices will not be protected even after the chosen encryption tool is fully implemented[8]. Reasons for not being able to achieve 100% compliance include:
    - Some devices lack the required internal computing capacity to install this feature.
    - The current encryption tool is not compatible on some devices (e.g., Macintosh Computers).
    - Some business units have been permitted to purchase their leased mobile devices after they received a replacement unit. This in effect nullifies the City's original strategy to replace older mobile devices as they came up for renewal, thereby ensuring that all mobile devices would have been encrypted within a three-year cycle. At the conclusion of this audit, IT advised the OCA of the following: "Information technology Branch confirms that our current standard practice is not to allow lease buy-backs of mobile devices at the end of their lease periods. There may be rare exceptions to this when a piece of hardware is bought-out as the application running on it cannot run on the new model." Mobile devices that were purchased in the past continue to be at risk if personal information is stored on them.
    - Some mobile device users have enquired about the process for seeking exemptions from having the encryption tool installed on their mobile devices. IT has advised that none have been granted an exemption.

Screen Saver Password Protection: The Commissioner uses strong words like "must have" and "cannot be disabled" regarding this specific control. There are 671 City employees (not limited to mobile device users) with access levels that permit them to disable this control. If disabled, when these users sign on to a mobile device, then the mobile device does not have screen saver password protection in place. Within this population, there is a subset of 62 full-time laptop users that have access levels that permit them to disable screen saver password protection. The City recently extended its screen saver lockout period from 15 to 60 minutes for all computing devices. International standards[9] recommend significantly shorter lockout times depending on the sensitivity of the data (from five minutes for highly sensitive data to 30 minutes for other data). The City's current setting of 60 minutes places the City at risk. Given that entering a password takes less than 7 or 8 seconds, screen saver lockouts should be set at periods consistent with the sensitivity of the data on the machine.

Remote Access: Current City guidance for using remote access to corporate data and applications places onus on the user to determine which method is most appropriate and how to use it properly. The Office of the Information and Privacy Commissioner of Alberta has ruled that it is not reasonable to count on non-technical employees to understand technical requirements and that controls: (a) should be implemented at the

[8] **Data Obtained From IT during the Audit (July 15, 2009):** There were a total of 1239 mobile devices, of which 137 could not be encrypted (i.e., 79 Toughbooks, 19 Macs, and 39 devices with storage capacity limitations).

[9] **Information Systems Audit and Control Association (ISACA);** *Enterprise Wide Identity Management (Managing Secure and Controllable Access in the Extended Enterprise Environment)*, 2003

enterprise level based on a risk analysis and (b) should be centrally managed. The remote access methods currently available in the City include:

- Outlook Web Access: This method is not in compliance with the required internal control because opening email attachments results in leaving a copy of any attached document on the user's remote device. This then requires the user to erase the documents if they happen to contain personal, confidential or sensitive information.
- Remote Web Access: Using this method to access City data leaves information on the data servers. However, it also results in leaving a copy of the document on the user's remote device. Again this requires the user to erase the documents if they happen to contain personal, confidential or sensitive information.
- Citrix Secure Gateway: Using this method, all data remains inside the City data servers, and the data is not copied on the user's remote device. This method, is fully compliant with the technical control requirement, and is recommended by Information Technology Branch (ITB). We have been advised by ITB that there may be significant cost associated with an enterprise-wide remote access solution.

In general, users have a false sense of security when they "delete" a file that may contain sensitive or personal information. "Deleting" a file does not actually remove the file from the computer. In order to fully erase a file, special software must be used that completely overwrites the disk space occupied by the file multiple times using techniques that destroy the data. It is not reasonable to expect the average user to know this or to know how to obliterate files downloaded to their mobile device. Encryption is one way to ensure that deleted files will not be easily recoverable. Current administrative directives need to clarify the "how to" requirements with deleting and/or erasing files with personal information.

In our opinion, the City does not have reasonable *technical controls* in place to protect personal information on mobile devices. Areas requiring remedies include encryption, screen saver password protection, and remote access. Effective implementation of enhanced *technical controls* will mitigate the chance of a privacy breach from occurring and associated costs that follow during the subsequent investigation process.

5.2.3. Are there reasonable *administrative controls* for protecting personal information on mobile devices?

Implementing administrative controls can be viewed as a proactive approach to responding to privacy risks that are overarching from a corporate perspective and involve dealing with people. The following table summarizes our assessment of the City's administrative controls against the prescribed Office of the Information and Privacy Commissioner's requirements. It is followed by a discussion of our observations and analysis.

Compliance to Prescribed Office of the Information and Privacy Commissioner of Alberta Standards for Administrative Controls

Description Of The Required Administrative Controls	✓ Criteria Met OR ✗ Criteria Not Met	
	Yes	No
Formal corporate direction that states that personal information data on laptop and tablets must be limited to what is necessary and that the data may only be stored for as long as necessary to complete the immediate task.	✓	
Formal corporate direction that makes reference to the fact that data should be permanently deleted once it is no longer required.	✓	
Formal corporate direction to require regular process audits to ensure that employees' access to personal information is limited to information for the performance of the functions and duties associated with each position.		✗
Formal corporate direction to require the conduct of ongoing random laptop and tablet audits to ensure compliance with laptop/tablet policy.		✗
Formal corporate direction to explicitly require Privacy Impact Assessments (including assessment of security risks) before implementing proposed operational practices involving mobile computing devices.		✗
Formal corporate direction to explicitly provide training (on an enterprise-wide basis) for all employees on how to protect personal information when using laptops/tablets. This training would include education sessions, personal information policy, and security awareness training.		✗
Formal corporate direction that the personal information policies for mobile devices are required to be read by every employee and states that there are consequences for violation.		✗
Formal corporate direction to require a periodic check of policies against practice to ensure they reflect reality and remain effective.		✗

A common theme is that the current administrative directives are silent on many of these criteria. A brief discussion of the identified control issues is presented below:

Process Audit: This type of management audit would assess access controls and permissions for personal information residing on electronic files. Employees' access to personal information must be limited to information required to perform their assigned functions and duties. Conducting a process audit can also identify new privacy risks (e.g., granting permission to a mobile device recovery vendor to have access to both view and recover files from a stolen device). Once a new privacy risk has been identified, an appropriate cost-effective mitigation measure needs to be developed, implemented and then audited to ensure effective implementation and compliance.

Laptop and Tablet Audit: This type of management audit would be conducted on a random basis to assist in evaluating compliance with the City's entire set of administrative directives. In the majority of investigation files we reviewed, we observed numerous examples of non-compliance issues. These directives currently place significant onus on supervisors to ensure full compliance. However, supervisors have not been:

- Trained to understand the importance of internal controls surrounding personal and sensitive information and how to appropriately exercise their responsibilities;

- Provided with a support structure to assist with administering the processes required by the administrative directives;
- Provided access to a system or network where they can seek guidance to assist in interpreting or applying new internal controls;
- Provided guidance on what to do when they find a non-compliance issue; and
- Advised of how, when, and to whom they should report the results of their findings.

As stated earlier, the Office of the Information and Privacy Commissioner has made it clear through its investigative reports that although an organization may have policies in place regarding laptop security, if employees do not comply with those policies, the organization is still accountable.

Privacy Impact Assessment: A Privacy Impact Assessment (PIA) is a formal tool that ensures that privacy is appropriately considered when implementing changes that involve either operational changes or changes involving technology and personal information. The two primary purposes of Administrative Directive A1433A, *Privacy* (June 11, 2004) are to:

- Ensure compliance with FOIP privacy provisions, and
- Ensure the completion of PIA whenever a system involving personal information is being developed or substantially changed.

Historically, the City has focused on major systems under development or undergoing major change, to the exclusion of operational practices. The City's PIA tool (developed by the Privacy Commissioner) needs to also be used to evaluate operational practices as they undergo significant change.

Training: Historically, the City has undertaken some communication to raise employee awareness of privacy issues related to mobile devices. New initiatives are being planned to further provide more in-depth training about privacy and relevant internal control requirements. Specific examples include:

- The Chief Information Officer has committed to develop a new over-arching security administrative directive. One element of this planned directive will address responsibilities around security measures, training, and ongoing communication.
- The FOIP Steering Committee is considering an enhancement to the City's various privacy directives. As part of this work, they are also planning for effective training and communication and methods of ensuring compliance.

In our opinion, related training initiatives are not effectively coordinated, organized or controlled primarily because there is neither an assigned process owner nor the assignment of accountability for delivering results, and ensuring the achievement of intended outcomes. Fundamentally, corporate training (and/or employee orientation) must be simple enough so that employees get the relevant messages in a clear and concise manner.

Assessing Compliance with Administrative Directives: There is currently no process in place to ensure that employees who work with personal and/or sensitive

information have read and understood the various administrative directives (see Section 2.2). For example, Administrative Directive A1444, *Protection of Mobile Sensitive Data* states that, "Employees may be subject to disciplinary action, up to and including dismissal, for violation of this Directive." However, we found no evidence in our review of the contents of investigation files from the last four years that potential violations were being assessed or acted upon. Current directing measures do not clearly identify who has the ultimate responsibility and accountability for dealing with non-compliance issues.

The results from detailed management privacy process audits and management random audits of laptops and tablets once implemented should be used to further assess practices against the City's applicable administrative directives to ensure they remain effective.

In addition, roles, responsibilities, accountabilities and authority for protecting personal information on mobile devices are not clearly defined. Current directing measures have various individuals (e.g., General Managers, Supervisors, FOIP Head, mobile device users, etc.) and functional areas (e.g., FOIP Steering Committee, Information Management Council, Information Technology, etc.) providing some guidance. This decentralized approach ultimately results in lessened accountability. We believe that this decentralized approach to protecting personal information contributes significantly to the gap we observed between the City's framework and actual practices against the audit criteria requirements.

In our opinion, the City does not have reasonable *administrative controls* in place to protect personal information on mobile devices. Areas requiring remedies include conducting management process audits; performing management laptop and tablet audits; conducting privacy impact assessments; training mobile device users; ensuring that employees understand relevant bylaws, policies, and directives and recognize that there are consequences for violations; and periodically assessing policies against practices. Effective implementation of enhanced *administrative controls* will mitigate the chance of a privacy breach from occurring and associated costs that follow during the subsequent investigation process.

Recommendation 1	Management Response and Action Plan
The OCA recommends that the General Manager of Corporate Services develop a detailed and comprehensive corporate implementation plan to respond to the audit results presented herein. The plan needs to: • Enhance corporate safeguards surrounding physical controls, technical controls, and administrative controls for mobile devices carrying personal information to ensure that reasonable protection against unauthorized access is provided if the mobile device is stolen or reported missing. • Develop an overarching framework that clearly articulates roles, responsibilities, accountabilities, and authority to ensure that corporate processes effectively achieve the desired outcome and are in compliance with FOIP requirements.	**Accepted** Comments: Several controls are being deployed to laptop and desktop computers in order to enhance security, of information and assets. The Chief Information Officer (IT Branch Manager) is finalizing the implementation of encryption technology for laptop computers. The Chief Information Officer is also currently implementing a 15 minute screen saver password lock for all laptop and desktop computers. The Chief Information Officer will incorporate the recommendations from this report into the IT Security Program. **Planned Implementation:** The IT Security Program will be complete by June 2010 and will include an implementation plan. **Responsible Party:** Chief Information Officer

5.3. Investigation Process for Lost or Stolen Laptops & Tablets

The table below presents estimated trend data for the number of missing or stolen devices and the number of investigations undertaken. The data is presented as estimated as there is no source where we could confirm the accuracy and completeness of the information. The Information Technology Branch does not maintain an inventory list of mobile devices at the beginning of the year, and at the end of the year, nor is there an annual reconciliation between these lists. Accurate inventory of mobile devices (as a corporate asset) should be maintained at all times. As reported earlier and shown in more detail below, the loss rate is currently estimated at 12 mobile devices per year (or one mobile device per month). Only 50% of the incidents were formally investigated. The City's process should ensure that all devices reported missing or stolen, are investigated. Corporate Services should ensure that the annual reconciliation process of mobile device inventory also aligns with the actual number of investigations (mobile devices) completed. All numbers must reconcile at year end, and through this annual activity, accurate numbers would then be available. There was only one investigation file that determined the nature of the information that was on the mobile device. Information Technology and FOIP staff members determined that it contained personal information (resumes). All other files were silent relative to the existence of personal information. Accordingly, no estimate can be made of the number of stolen or missing devices that actually had personal information on them.

Estimated Trend Data for Missing / Stolen Devices and Investigations Undertaken

	2005	2006	2007	2008	Overall Trend
Total Number Of Devices Missing or Stolen **(Less the number of devices recovered)** **Net Loss**	**14** **0** **14**	**15** **0** **15**	**12** **2** **10**	**11** **2** **9**	52 4 12/year
• Average Devices Per Month (Missing or Stolen)	1.17	1.25	0.83	0.75	1.00/month
Number Of Investigations Undertaken: ▪ **(Number Of Devices Involved)** ▪ **(% Of Missing/Stolen Devices Investigated)** **(I.e., number of devices involved / total number of devices missing or stolen)**	**1** (1) (7%)	**2** (6) (40%)	**4** (9) (75%)	**8** (8) (73%)	15 24 (50)%

Note:.Includes investigations conducted by either Corporate Security or Risk Management or both (Law Branch).

Failure to fully evaluate, and assess the information on lost or stolen mobile devices and investigate the loss is primarily due to the following:

- There is no established process owner or reporting procedure for addressing the loss or theft of mobile devices.
- Corporate Security takes the lead into a mobile device theft investigation, but only if they are made aware of the incident. There is corporate direction (Administrative Directive A1444: Protection of Mobile Sensitive Data) that states: "Employees must report all lost or stolen Mobile Data Storage immediately to Corporate Security, along with the list of sensitive data documents." In some cases, the employee may not know if their mobile devices (refer to Remote Access methods on Page 11) has

sensitive data because of how the technology works. These two non-compliance issues require management's attention if all losses are to be investigated.
- Risk Management is only involved in a very small percentage of losses and thefts that are investigated. This is because most mobile device losses and thefts are under the $5,000 deductible (typically a single device). Risk Management is involved when multiple devices are stolen in a single incident.
- Existing directives do not require anyone to assess personal or sensitive information loss as part of the protocol for reporting loss or theft of mobile devices. This should be decided by using FOIP subject matter experts.

The City does not have a comprehensive and formally documented management framework for reporting and dealing with all missing or stolen devices in a timely manner. The current framework consists of an "informal" 2 page flow chart. Given both the estimated number of mobile devices stolen each year, and the significant costs incurred, a coordinated and effective response strategy is necessary. Specifically the following elements need to be undertaken and formalized:

- Assignment of a corporate process owner to ensure that the investigation protocol is fully developed and implemented. The assigned owner would be accountable for periodically reviewing and updating the process and for ensuring compliance with requirements through periodic, structured management reviews or audits.

- Enhancing the investigation process effectiveness by describing the roles, responsibilities, and accountabilities of key participants involved (Information Technology, Corporate Security, Risk Management, Human Resources, Edmonton Police Services, Corporate FOIP, Users, Inside Information, Data Delete Administrator, and others as required).

- Development of an effective communication strategy to ensure that all current and future mobile device users are advised and periodically re-advised of the required process to follow when a mobile device is lost or stolen. The communication strategy would need to emphasize that reporting must be timely and that employees have both the duty and obligation to cooperate fully with investigators.

- Determine how best to maximize the functional capabilities of a software tool that is used to facilitate mobile device recovery and/or data deletion. This tool has been in use since mid 2006 and is currently on all new mobile devices. The City has been successful in some cases in recovering devices (2 in 2007 and 2 in 2008). The tool could also be used for forensic detection, inappropriate software monitoring, missing device reporting, partial software delete, etc. These features need to be reviewed, and then included in the City's standard software installation as required.

- Enhance Risk Management investigations as they are involved in claims management relating to stolen or missing mobile devices. They settle losses in excess of the department deductible of $5,000. They are also involved in evaluating the risk exposure incurred by the loss of personal information or sensitive data. Risk

Management advised us that this exposure is covered by the City's municipal errors and omissions liability insurance. However, this form of insurance is becoming more difficult and costly to obtain. Risk Management has initiated steps to promote greater consistency in its internal practices when handling such cases. Risk Management tends to be involved only with cases that involve multiple devices during a single theft incident because departments may not notify them if the replacement value is less than the $5,000 deductible. In the future, Risk Management should be involved in assessing all lost or stolen devices and evaluate the costs that may be incurred as a result of information loss.

- Enhance Corporate Security investigations to determine the reason for each reported loss or theft of a mobile device in order to recommend remedial actions and help avoid similar losses in the future. Potential learnings from each case should be shared with the appointed process owner to ensure continuous improvement of the corporate-wide protocol. We noted three investigations where Corporate Security's attempts to conduct an effective investigation were hampered by employees not cooperating fully in the investigation: one employee was not willing to file a police report, a second employee was initially reluctant to provide a statement to the investigator, and the investigator encountered significant push back from the third employee. Employees must be advised that they are required to cooperate with the investigator.

- Strengthen the current *Privacy Breach Directive* to ensure it is more thorough and consistent with leading practices used by the Privacy Commissioners of both Alberta and Canada. Key elements of these latter two frameworks include:
  - Breach containment and preliminary assessment (immediate steps to limit the breach);
  - Evaluate the risks associated with the breach (determine the types of information involved, cause and extent, individuals affected, and foreseeable harm resulting from the breach);
  - Notification (determining when, how, and who to notify; who should do the notification; what should be included in the notification; and identifying any others to contact); and
  - Action to prevent future breaches (develops and implements a prevention plan and subsequently audits the prevention plan to ensure effective implementation).

It is critical that FOIP and Information Technology knowledge be applied in every mobile device loss or theft investigation to formally determine whether or not the lost or stolen device contained personal information as determined by FOIP.

In our opinion, the City needs to develop a comprehensive Administrative Directive and supporting procedures (or an appropriate alternative) to provide corporate direction on the process to be followed whenever a laptop or tablet is missing or stolen. In the absence of such a directive and procedures (and verified compliance with it) there is no assurance that appropriate due diligence will be taken when laptops or tablets are either missing or stolen.

Recommendation 2	Management Response and Action Plan
The OCA recommends that the General Manager of Corporate Services develop comprehensive directing measures (or an appropriate alternative) that details the roles and responsibilities related to mobile devices and the formal corporate process to be followed when a laptop or tablet is stolen or missing. At a minimum, the directive should include the following attributes: • Assignment of a process owner; • Articulate roles, responsibilities, and accountabilities of key participants; • Develop an effective communication strategy to inform all mobile device users of process requirements and user responsibilities; • Maximize functional capabilities surrounding the full deployment of mobile device recovery and/or data deletion software capabilities; • Enhance investigation protocols for Risk Management and Corporate Security; and • Strengthen the privacy breach investigation framework in accordance with leading practices.	**Accepted** Comments: The Chief Information Officer, on behalf of the General Manager Corporate Services and in partnership with the City Solicitor will develop an administrative directive addressing the attributes within the recommendation. **Planned Implementation:** Administrative directive to be complete and ready for approval by June 2010. **Responsible Party:** Chief Information Officer

6. Conclusion

The objective of this audit was to provide assurance that appropriate safeguards (consistent with best practices) are in place to protect personal information on the City's mobile devices (i.e., laptop and tablet computers).

The Office of the Information and Privacy Commissioner of Alberta recommends three layers of security and safeguards in order for public bodies to discharge there FOIP obligations to protect personal information on mobile devices. They include physical controls, technical controls, and administrative controls. With a layered security approach, each layer offers an incremental level of protection to the electronic data. Combined, reasonable protection against unauthorized access is provided if the device is stolen or reporting missing. Only when there are reasonable safeguards surrounding all three controls, could we conclude that the City of Edmonton has met its duty to safeguard personal and sensitive information on mobile devices in its custody, as required by section 38 of FOIP.

Our overall assessment for the three key sets of internal controls is:

- The City has implemented reasonable *physical controls* to protect personal information on mobile devices. We have suggested some opportunities for improvement to enhance these controls. (Section 5.2.1)
- The City has not implemented reasonable *technical controls* to protect personal information on mobile devices. (Section 5.2.2)
- The City has not implemented reasonable *administrative controls* to protect personal information on mobile devices. (Section 5.2.3)

The absence of clarity in roles, responsibilities, accountabilities and authority is the primary root cause of the gaps between internal control requirements and actual practices identified in this audit.

The potential for fraud and identify theft is real. A 2009 report titled *Best Practices: Mobile Device Security*[10] stated:

> It is tempting to think that thieves are most interested in the physical device they are stealing, however the reality is that increasing the information on the mobile device is far more valuable to thieves rather than the device itself. As Ontario Information and Privacy Commissioner Anne Cavoukian commented:
>
> > There is no way of distinguishing one kind of theft from another. Personal information stored on stolen devices can be used for purposes such as fraud and identity theft – problems that have reached epidemic proportions throughout North America. And with the movement of organized crime into this area, the problem takes on a greater and more sinister complexion.

[10] ***Best Practices: Mobile Device Security***, Office of the Saskatchewan Information and Privacy Commissioner, May 29, 2009

The City of Edmonton, as a steward of personal and sensitive information, must take as many measures as reasonably possible to safeguard the information in its care against such risks as unauthorized access, collection, use, disclosure or destruction. Effective implementation of enhanced *physical controls, technical controls, and administrative controls* will mitigate the chance of a privacy breach from occurring and associated costs that follow during the subsequent investigation process.

This audit also considered the incidence of stolen or missing devices and the investigative process that follows. The corporate investigative process when a mobile device is reported missing or stolen needs to be strengthened in several areas. This will ensure timely and effective investigation of this corporate asset. (Section 5.3)

Effective implementation of the two audit recommendations by the City will ensure that appropriate safeguards are in place to protect personal information on laptops / tablets. Although the specific observations, analysis and recommendations are directed towards laptops and tablets, the go forward corporate strategy should ensure that all mobile devices are included.

Acknowledgements
We thank the management and staff of the organizational units that participated in this audit. They include:

- Information Technology Branch (Office of the Chief Information Officer; Information Technology Security; Information Technology Planning and Architecture; Information Technology Contracts, License, & Vendor; and Customer Support),
- Law Branch (FOIP Legal Expert),
- Corporate Security,
- Risk Management,
- City Clerk (FOIP Manager), and
- FOIP Steering Committee Members.

7. Appendix 1 - Definition Of "*Personal Information*" In the FOIP Act

Section 1 (Definitions)

Subsection (n) "*personal information*" means recorded information about an identifiable individual, including:

(i) The individual's name, home or business address or home or business telephone number,

(ii) The individual's race, national or ethnic origin, colour or religious or political beliefs or associations,

(iii) The individual's age, sex, marital status or family status,

(iv) An identifying number, symbol or other particular assigned to the individual,

(v) The individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

(vi) Information about the individual's health and health care history, including information about a physical or mental disability,

(vii) Information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,

(viii) Anyone else's opinions about the individual, and

(ix) The individual's personal views or opinions, except if they are about someone else.