EDMONTON

ADMINISTRATIVE PROCEDURE

TITLE	NUMBER	*A1444*
PROTECTION OF MOBILE SENSITIVE DATA	DEPARTMENT	*OFFICE OF THE CITY MANAGER*
	DELEGATED AUTHORITY	*FREEDOM OF INFORMATION AND PREVENTION OF PRIVACY ACT (FOIP) S38*
	CONTACT	*CORPORATE FOIP ANALYST 496-8159* *CORPORATE SECURITY 496-4981* *I.T. SECURITY 496-8114*
DEFINITIONS	DATE	*MAY 24, 2007*

City – The City of Edmonton as defined in Bylaw 12100, Freedom of Information and Protection of Privacy Bylaw.

City Information Banks – These refer to all forms of electronic information stored on City server computers.. Examples include (but are not limited to) the electronic mail system, application databases, private and shared file directories, document repositories, knowledge management repositories.

City Premises – This refers to any work space used by Employees for the purposes of conducting City business.

Disclosure – Disclosure means intentionally or unintentionally to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or give information by any means to someone. It includes oral transmission of information by telephone, or in person; provision of information on paper, by facsimile or in another format; and electronic transmission through electronic mail, data transfer or the Internet.

Employee – This means an individual employed by the City, including those employed on a personal services agreement, but does not include volunteers, those retained by the City on a professional services agreement, civic agency, board or committee members not employed by the City, elected officials and their assistants.

Encryption Solution – This means one of the City-approved technical solutions for converting information into unreadable forms (via industry-standard methods) which are essentially impossible to translate back into readable form without using the correct original encryption key.

THE CITY OF Edmonton

TITLE	NUMBER	*A1444*
PROTECTION OF MOBILE SENSITIVE DATA	DATE	*MAY 24, 2007*

FOIP – The *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25.

Mobile Data Storage – 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, USB flash memory sticks, portable disk drives, diskettes, data tapes, CDs & DVDs (various types). NOTE: Mobile Data Storage might be City assets, but there could be personally owned Mobile Data Storage which is being used to store City information.

Mobile Sensitive Data – Sensitive Data that is copied or moved off of City Information Banks in any form. This is commonly copied onto Mobile Data Storage, but could include many other situations (including onto desktop computers, or sent outside the City via e-mail).

Non-City Computers – Any computer not owned or leased by the City but which is used (even temporarily) to access or work with City information.

Personal Information – This is recorded information about an identifiable individual, including the individual's name, home or business address or home or business telephone number, the individual's race, national or ethnic origin, colour, religious or political beliefs or associations, the individual's age, sex, marital or family status, information about the individual's educational, financial, employment or criminal history, anyone else's opinions about the individual, etc. See s.1(n) of FOIP.

Remote Access Methods – These are the City-approved methods of electronically accessing data from City Information Banks from outside City Premises (via remotely connecting and communicating). Examples include (but are not limited to): Outlook Web Access, Remote Web Access, Citrix Secure Gateway, and other virtual private network solutions approved at the City.

Sensitive Data – This is a general term for electronic information not allowed to be released to any members of the public. Sensitive Data includes (but is not limited to) Personal Information, business information related to a third party, draft documents, or other information deemed to be confidential (and exempted or excluded from release under FOIP). Examples of high risk Sensitive Data would include health information, payroll information, credit/debit card or banking information, and social services records.

PROCEDURES

General

Protection from unauthorized Disclosure of Sensitive Data located on Mobile Data Storage is the responsibility of each Employee. Wherever possible, Employees should avoid the risks of creating Mobile Sensitive Data by leaving the data on City Information Banks. (Instead, access the data directly and if necessary use Remote Access Methods to work with the information from outside City Premises.)

Protecting Mobile Data Storage and Mobile Sensitive Data

To reduce the risk of theft or loss of Mobile Data Storage and Mobile Sensitive Data, Employees must follow mandatory security guidelines at all times. (See Guidelines)

TITLE	NUMBER	*A1444*
PROTECTION OF MOBILE SENSITIVE DATA	DATE	*MAY 24, 2007*

Prior to using any Sensitive Data, Employees must determine the level of risk, i.e. the impact to the City if that data were to undergo inadvertent Disclosure to unauthorized parties. Depending on the level of risk of Sensitive Data, additional protections may need to be followed where appropriate. For high risk Sensitive Data, additional mandatory guidelines must be followed. (See Guidelines)

Supervisors are responsible for assisting Employees in the assessment of risk and may need to contact their Department FOIP Coordinator, Corporate Security Advisor, IT Security Architect or department management for advice.

Employees must consult with their Supervisor in advance when they intend to move or copy Sensitive Data from City Information Banks. Expected time-periods for use of Mobile Sensitive Data must be explicitly identified and discussed. Use of the attached Mobile Sensitive Data Form is strongly recommended.

Employees are responsible for maintaining a list of all Sensitive Data contained on Mobile Data Storage, to be used in case the data gets lost or stolen. All Mobile Sensitive Data is to be considered a temporary copy, and Employees must delete it in a timely manner.

Reporting Losses of Mobile Data Storage

Employees must report all lost or stolen Mobile Data Storage immediately to Corporate Security, along with the list of Sensitive Data contents. If Personal Information was present on the lost or stolen Mobile Data Storage, also refer to the Privacy Breach Directive A1445.

Compliance

Employees may be subject to disciplinary action, up to and including dismissal, for violation of this directive.

Work unit Supervisors are encouraged to conduct ongoing reviews to ensure that Employees' access to Sensitive Data is appropriately limited and random checks of Mobile Data Storage (especially laptops) to ensure compliance with this Directive.

TITLE	NUMBER	A1444
PROTECTION OF MOBILE SENSITIVE DATA	DATE	MAY 24, 2007

GUIDELINES

These guidelines might not necessarily represent a complete list of protections appropriate to your particular situation.

MANDATORY Guidelines for use of Mobile Data Storage

REGULARLY, ONGOING:

- When leaving work at the end of the day, secure Mobile Data Storage in lockable cabinets or drawers in your office.
- Regularly check that you are still in possession of all Mobile Data Storage, in order to identify as early as possible any assets you may have lost.
- Regularly copy updated City information back to City Information Banks. Never keep the only copy of any data or document on Mobile Data Storage.

PRIOR TO TRANSPORTING MOBILE DATA STORAGE OUTSIDE CITY PREMISES:

- Mobile Data Storage must not be labeled with any identifier that would identify it as owned by the City of Edmonton. Either have no label at all, or use only a phone number or generic return address (e.g. a P.O. box number or a building location which is not wholly City offices).
- At the start of each trip when traveling in motor vehicles, secure Mobile Data Storage in a lockable trunk or storage compartment in the vehicle if at all possible. Do not transfer Mobile Data Storage to a trunk at the destination of the trip (as that will be visible to people nearby). Never leave Mobile Data Storage in the passenger area of a motor vehicle.

WHILE MOBILE DATA STORAGE IS OUTSIDE CITY PREMISES:

- Keep Mobile Data Storage with you at all times when traveling on foot in public places. This includes going into restaurants and washrooms, and while shopping.
- Always bring Mobile Data Storage with you as carry-on luggage, when traveling on airlines, trains, buses or other public transportation.
- Never leave Mobile Data Storage unattended, even for a few seconds. Bring them with you into washrooms, or leave them for short periods of time in the explicit care of responsible Employees traveling with you.

TITLE	NUMBER	*A1444*
PROTECTION OF MOBILE SENSITIVE DATA	DATE	*MAY 24, 2007*

These guidelines might not necessarily represent a complete list of protections appropriate to your particular situation.

MANDATORY Guidelines for ALL Mobile Sensitive Data

REGULARLY, ONGOING:

- Regularly review the contents of Mobile Data Storage to identify and then erase Sensitive Data that is no longer needed there.
- Regularly list or print contents of Mobile Data Storage, especially noting the Mobile Sensitive Data you have chosen to carry with you. Keep this list physically separate from the Mobile Data Storage. This list will be critical in case the Mobile Data Storage gets lost or stolen.
- Regularly delete temporary copies of any City information that you no longer need from Non-City Computers.

PRIOR TO TRANSPORTING SENSITIVE DATA FROM CITY INFORMATION BANKS:

- Never store any Sensitive Data on types of Mobile Data Storage (especially laptop and tablet computers) which are highly targeted for theft.
- Regularly seek confirmation from your Supervisor when Sensitive Data is to be kept on Mobile Data Storage beyond the originally anticipated time period.

WHILE SENSITIVE DATA IS LOCATED ON MOBILE DATA STORAGE:

- Always store Mobile Sensitive Data using an Encryption Solution. A password alone is not enough. Where possible, store Sensitive Data only on Mobile Data Storage which come with built-in Encryption Solutions. Otherwise, you must take steps to use a City-approved Encryption Solution yourself to hide the Sensitive Data before you store it there. It is prohibited for Employees to disable or attempt to disable Encryption Solutions.
- Keys and/or passwords used with Encryption Solutions must be recorded and kept in a secure location, and only communicated to others securely. If this is not followed, the information will become permanently inaccessible if the keys or passwords are forgotten.
- Delete copies of Sensitive Data immediately when your need to use them has ended. This applies not only to City-acquired Mobile Data Storage but also to Non-City or personally-owned Mobile Data Storage.
- If establishing a business process where Sensitive Data is to be regularly copied or communicated by Employees, a Privacy Impact Assessment is mandatory.

These guidelines might not necessarily represent a complete list of protections appropriate to your particular situation.

MANDATORY Guidelines for HIGH RISK Mobile Sensitive Data

REGULARLY, ONGOING:

- Supervisors are to conduct ongoing reviews to ensure that Employees' access to high risk Sensitive Data is limited to information required for the performance of the functions and duties associated with each position.
- Supervisors are to conduct ongoing random checks of the higher risk types of Mobile Data Storage (e.g. laptops) to ensure compliance with this Directive.

PRIOR TO TRANSPORTING HIGH RISK SENSITIVE DATA FROM CITY INFORMATION BANKS:

- Be sure you actually need to copy high risk Sensitive Data off City Information Banks. Except in very unusual circumstances, leave high risk Sensitive Data there, and use Remote Access Methods to work with the information.

WHILE HIGH RISK SENSITIVE DATA IS LOCATED ON MOBILE DATA STORAGE:

- When working at home with high risk Sensitive Data using City laptops or tablet PCs, use a cable lock or other secure device to provide additional protection.
- Simply do NOT use Non-City Computers at all when using high risk Mobile Sensitive Data.

FREQUENTLY ASKED QUESTIONS

Why are City Information Banks so much more secure than my laptop?

Server computers are typically on City Premises, and are within computer facilities that have additional physical security protections. The City also has various network protections. Laptops go anywhere, are in demand, and can be stolen within seconds.

City laptops have a logon password. Why isn't that enough protection?

The Windows logon password can be bypassed using several widely-known methods, enabling a thief who seriously wants to do so to read the contents of the laptop hard drive.

How do I know whether the data I work with is Sensitive Data or not?

Consider what the worst consequences could be if the data were to be read by members of the public, or someone practicing identity theft. Then, if you are still unsure, discuss with your Supervisor. Draft versions of documents are not normally released to the public, and could be considered Sensitive Data. Other common Sensitive Data include: performance reviews, tender information, and contracts.

I don't work with Sensitive Data. Do I still have to remove all the data from my laptop?

Sensitive Data must always be stored encrypted on laptops or other Mobile Data Storage. If you are completely sure that you do not have Sensitive Data, and have confirmed that with your Supervisor, then storing that data on your laptop's hard drive may be tolerated.

What tools can I use to protect (i.e. encrypt) Sensitive Data when using CDs or diskettes, or even laptops?

Every City computer comes with the WinZip software and it is easy to use. WinZip version 9 or higher has an option you must select to encrypt a WinZip archive using a password and encryption which will adequately protect Sensitive Data on any Mobile Data Storage. (Winzip without a password does not do encryption.)

Can I still use my old non-encrypted USB drive or memory stick?

Only store Sensitive Data using an Encryption Solution. Use only the City-standard encrypted memory sticks. If they do not require a password key to get in, do not use USB storage devices for City data. That includes personally-owned ones.

Why not put a return address on laptops?

Identifying the City as owner may encourage someone who finds a laptop to try to access the information stored there. From a law enforcement point of view, the serial number adequately identifies the laptop.

What if I have to use an airport kiosk PC or an internet café to connect back to the City?

That's okay for checking your e-mail. Do not use Non-City Computers for accessing or updating Sensitive Data. If you absolutely have to access Sensitive Data on a Non-City PC, be doubly sure that no copy of Sensitive Data is left behind when you are done. Any time you use a PC in an airport kiosk or internet café, also be sure you completely logoff and close any active browser windows you were using. Restart the PC when you leave, if possible.

My job requires me to work with some high-risk Sensitive Data. What other precautions should I take?

Assuming you have your Supervisor's approval to copy the high-risk Sensitive Data, only store the high-risk Sensitive Data on an encrypted USB memory stick. And only use City computers when handling high-risk Sensitive Data.

I am taking a City laptop on a business trip. Beyond the minimum guidelines, what other precautions should I take?

Consider using a cable lock or other locking device to provide additional protection when you use a laptop in a hotel or meeting room, but also consider using a cable lock when using a City laptop at home.

I have heard that laptops have even been stolen from people while standing in line in an airport. What can I do to help avoid that?

When standing in line, loop the carry strap of the laptop case around your leg when you put the case down. That way, you will be immediately aware if somebody tries to grab it. For smaller types of Mobile Data Storage (e.g. PDAs and Blackberrys) keep them hidden from view while not in actual use.

Mobile Sensitive Data Form

Employee:	**Date:**
Supervisor:	
Name of database or Title of information copied:	
Does your job require you to have this information on a portable device? Yes / No	
Expected Time Period of Use: **Starting date:**	**Ending date:**
Type of Mobile Data Storage to be used:	
☐ **Laptop**	☐ **Portable hand held or PDA**
☐ **Tablet**	☐ **Blackberry**
☐ **Diskettes**	☐ **Data tapes**
☐ **CDs**	☐ **DVDs**
☐ **USB Flash memory stick**	☐ **USB portable disk drive**
☐ **Other: (specify)**	
Type or Description of Information copied (list key data fields):	
Sensitive Data? Yes / No	**Privacy Impact Assessment Completed ? Yes / No**

Risk Level of Sensitive Data: (check the one that best applies)

☐ **High Sensitivity** (serious risk to citizen/employee or serious potential impact if inappropriately released) See the back side of this form for criteria to assist in the identification of High risk Sensitive Data.

☐ **Moderate Sensitivity** (lower risk to citizen/employee or moderate potential impact if inappropriately released) See the back side of this form for criteria to assist in the identification of Moderate risk Sensitive Data.

☐ **No Sensitivity** (has no personal information, and the data is already publicly available)

Comments on above or other risk factors involved:

Action(s) taken to protect copy of Sensitive Data (check any or all that apply)

☐ **Encryption Solution used**
Specify:

☐ **Additional physical security protection actions taken**
Specify:

☐ **Other actions, if any**
Specify:

Date updated information copied back to City Information Banks:

Date Sensitive Data erased:

THE CITY OF Edmonton

Additional Criteria to Consider in Assessment of Risk

Consider the following factors, and check all that apply.

High Sensitivity (serious risk to citizen/employee or serious potential impact if inappropriately released)

Disclosure of information could result in at least one of the following:

- ☐ Potential for physical harm to individuals; Increased public health risks
- ☐ Substantial financial loss to the City (including recovery costs, legislative penalties or civil liability) and/or to individuals affected
- ☐ Potential for some Infrastructure or asset destruction
- ☐ Loss or compromise of public confidence in COE
- ☐ Interference with ability to provide service

Moderate Sensitivity (lower risk to citizen/employee or moderate potential impact if inappropriately released)

Disclosure of information could result in at least one of the following:

- ☐ Some financial loss to the City (including recovery costs and effort/costs to inform parties) but not likely to individuals affected
- ☐ Potential for Infrastructure or asset degradation
- ☐ Embarassment to COE
- ☐ Temporary disruption to business area

No Sensitivity (has no personal information, and the data is already publicly available)

Disclosure of information will have no significant impacts. For example:

- ☐ Information is already available to the public, or is available to anyone upon request or for a small fee.
- ☐ Information is available elsewhere or comes from outside sources, and so can be replaced readily.

When ready, use the above to transfer the highest sensitivity risk level back to page 1 of the Form.