ADMINISTRATIVE DIRECTIVE

DIRECTIVE NUMBER: A1435

REFERENCE:
SMT August 1, 2002

ADOPTED BY:
City Manager

SUPERSEDES:
New

PREPARED BY:	Corporate Services Department, Law Branch	**DATE:**	August 1, 2002
TITLE:	**VIDEO SURVEILLANCE IN PUBLIC AREAS**		

Directive Statement:

The City of Edmonton recognizes the need to balance an individual's right to protection of privacy against the city's duty to promote a safe environment for all citizens, and to protect city property.

This directive is intended to assist departments in deciding whether collection of personal information by means of a surveillance camera is both lawful and justifiable, and if so, in understanding how privacy protection measures can be built into the use of a surveillance system.

It is recognized that each department has unique needs and practices. While these requirements will remain, it is necessary to standardize city procedures in order that all citizens have an expectation of consistency, regardless where the equipment is installed.

The purpose of this policy is to:

Develop a surveillance system policy that complies with the *Freedom of Information and Protection of Privacy Act.*

Ensure consistency of corporate surveillance measures.

These guidelines do not apply to covert or overt surveillance cameras being used as a case-specific investigation tool for law enforcement purposes or in contemplation of litigation. They are also not intended to apply to workplace surveillance systems installed to conduct surveillance of employees.

ADMINISTRATIVE PROCEDURE

DIRECTIVE NUMBER: A1435

AUTHORITY: City Manager

EFFECTIVE DATE: August 1, 2002

TITLE: Video Surveillance in Public Areas

1.0 Definitions:

1.1 City as referred to in this Directive, shall include all departments and offices which make up the City administration, as well as any agency of City Council which has agreed to be bound by this Directive.

1.2 Covert Surveillance refers to the secretive continuous or periodic observation of person, vehicles, places or objects to obtain information concerning the activities of individuals.

1.3 FOIP means the *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25.

1.4 Overt Surveillance refers to the non-secretive continuous or periodic observation of person, vehicles, places or objects to obtain information concerning the activities of individuals.

1.5 Personal Information is defined in section 1(1)(n) of FOIP as recorded information about an identifiable individual. It includes the individual's race, colour, national or ethnic origin; the individual's age or sex; the individual's inheritable characteristics; information about an individual's physical or mental disability; and any other identifiable characteristics listed in that section.

1.6 Privacy Impact Assessment (PIA) is a process that can be applied to any public body for the purpose of determining the level of protection and security afforded to personal information that is collected, used or disclosed in a new or modified information system. The security of information refers to the technical, physical and procedural measures taken to protect personal information from the time it is collected until a public body disposes of it.

1.7 Reception Equipment refers to the equipment or device used to receive or record the personal information collected through a surveillance system, including a video monitor.

1.8 Record is defined in section 1(1)(q) of FOIP as a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

1.9 Storage Device refers to a videotape, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

ADMINISTRATIVE PROCEDURE

1.10 Surveillance System refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces, public buildings or public transportation.

2.0 Responsibilities:

2.1 City Manager to:

a) approve this Directive and any subsequent amendments.

2.2 General Managers to:

a) ensure the requirements of this Directive are adhered to;

b) establish and maintain an internal reporting network relating to control mechanisms and advise the Director of Corporate Security;

c) budget for the costs of their video surveillance requirements;

d) ensure Privacy Impact Assessment are conducted on new surveillance initiatives and on significant upgrades to existing surveillance systems;

e) for each operating area, develop guidelines pertaining to retention period and storage for storage devices, and determining who shall have access to view storage devices;

f) inform the Director of Corporate Security of:

i) proposed changes to authorized video surveillance which may affect Corporate Security;

ii) proposed changes in internal reporting network relating to proposed installation of new surveillance system equipment that may be affected by this Directive.

2.3 City Auditor to:

a) conduct periodic audits to ensure compliance with this directive.

2.4 Director of Corporate Security to:

a) assist General Managers with the administration of this Directive;

b) ensure that any new legislation pertaining to the use of video surveillance is incorporated into this Directive, as required;

c) review all proposed changes to existing video surveillance systems and newly proposed systems to ensure that they meet all the requirements of this Directive;assist each operating area in the development of guidelines pertaining

to retention period and storage for storage devices and determining who shall have access to view storage devices.

2.5 Employees to:

a) review and comply with this Directive in performing their duties and functions related to the operation of a surveillance system;

b) attend training relating to this Directive, where available.

3.0 Procedures

3.1 Designing and Installing Surveillance Equipment

a) Reception equipment such as video cameras may be installed in identified public areas where surveillance is a necessary and viable detection or deterrence activity.

b) Reception equipment shall not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to protect external assets or to ensure personal safety. Cameras should not be directed to look through the windows of adjacent buildings.

c) Equipment shall not monitor areas where the public and employees have a reasonable expectation of privacy e.g. showers, restrooms.

d) Consideration should be given to the use of surveillance being restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance. Only authorized persons should have access to the system's controls and to its reception equipment.

e) Reception equipment should be in a controlled access area. Only the controlling personnel or those properly authorized in writing by those personnel should have access to the reception equipment. Video monitors should not be located in a position that enables public viewing.

3.2 Public Awareness Of Cameras

a) The public must be notified, using clearly written signs prominently displayed at the perimeter of surveillance areas, so the public has ample warning that surveillance is or may be in operation before entering any area under surveillance.

b) Unless the public has otherwise been made aware of surveillance cameras at a surveillance area, the main entrance of the area will display the following notice:

Surveillance cameras may be operating in <location of camera> to deter and/or detect criminal activity and for public security. The collection of

recorded camera images is authorized under section 33(c) of the Freedom of Information and Protection of Privacy Act (FOIP) Act. If you have any questions about this surveillance, contact <name of position> at <phone number>

c) In addition, the following sign will be displayed at the surveillance location:

Surveillance camera may be operating in this area to detect and/or deter unlawful activity (vandalism, theft) and for public security. For more information, contact <name of position> at <phone number>.

3.3 Limiting Use, Disclosure And Retention Of Personal Information

a) All storage devices that are not in use should be stored securely in a locked receptacle located in a controlled access area. All storage devices that have been used should be numbered and dated.

b) Access to the storage devices should only be by authorized personnel.

c) A logbook will be kept with regard to the use of each recording device. Storage Devices will only be removed when an incident occurs. The employee will take control of the storage device in question and secure it in a sealed envelope with the time and date of the seizure and initials of the employee on the seal of the envelope.

d) Written policies on the use and retention of recorded information should cover:

i) Who can view the information and under what circumstances.

ii) How long the information should be retained where viewing reveals no incident or no incident has been reported.

iii) How long the information should be retained if it reveals an incident.

e) If the surveillance system has been installed for public safety or deterrence purposes but detects possible criminal activity or non-compliance with or breach of a statute or bylaw that could lead to a penalty or sanction, the storage devices required for evidentiary purposes should be retained and stored according to standard procedures.

f) A storage device release form (Appendix A – Law Enforcement Disclosure Form) should be completed before any storage device is disclosed for Law Enforcement purposes.

g) An individual who is the subject of the information has a right to access to his or her recorded information. Access may be granted in full or in part depending upon whether any of the exceptions in FOIP apply and whether the excepted information can reasonably be severed from the record.

h) Old storage devices must be securely disposed of by shredding, burning or magnetically erasing the information

.

THE CITY OF Edmonton

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY

Law Enforcement Disclosure

Request for Disclosure under Section 40(1)(q) of the Freedom of Information and Protection of Privacy Act

Date:

In accordance with section 40(1)(q) of the *Freedom of Information and Protection of Privacy Act*, the

_____

Name of Public Body

requests disclosure of personal information pertaining to

_____

Name of Individual or Other Identifier

which may be generally described as:

_____

General Description of Information Requested

This information is required by this public body to assist in an investigation pursuant to:

Reference to a Federal or Provincial Statute or Local Public Body Bylaw by Section or Description of Purpose

2

3 Requesting Official

_____	_____
Name	Title
_____	_____
Signature	Badge Number *(if applicable)*

I, _____ ☐ consent to ☐ refuse this disclosure

Name of Disclosing Official

of personal information.

If disclosure has been authorized, the personal information bank(s) is:

_____

Name(s) of Personal Information Bank(s)

4 Authorized Disclosing Official

_____	_____
Name	Title
_____	_____
Signature	Name of Public Body

NOTE: This completed record may qualify for exception to disclosure under section 20 of the *Freedom of Information and Protection of Privacy Act*.