TORONTO CITY CLERK

Consolidated Clause in Administration Committee Report 4, which was considered by City Council on July 25, 26 and 27, 2006.

21a

City of Toronto Security Video Surveillance Policy

City Council on July 25, 26 and 27, 2006, amended this Clause by adding the following:

"That:

(1) the City Manager be requested to report to Council, through the Administration Committee, on the possibility of conducting a joint public meeting with the Toronto Police Services Board before the Board adopts a video surveillance policy;

(2) Council request the Toronto Police Services Board to direct the Toronto Police Service to consult with the City in the development of best practices and privacy principles before the Toronto Police Services Board adopts a video surveillance policy; and

(3) the Chief Corporate Officer be requested to research best practices in technology in other jurisdictions, including New York City, and make recommendations on appropriate measures to City Council, through the Administration Committee, within six month's time."

This Clause, as amended, was adopted by City Council.

City Council on June 27, 28 and 29, 2006, postponed consideration of this Clause to its next regular meeting on July 25, 2006.

The Administration Committee recommends that City Council:

(1) adopt the Security Video Surveillance Policy (including Appendices 1 to 6) in the report (May 15, 2006) from the Chief Corporate Officer, subject to amending the Security Video Surveillance Policy as follows:

(a) on page 3, under the heading "Responsibilities of All City Staff", insert the word "disclose", before the words "access or use information", so that it now reads as follows:

"All City Staff must adhere to the video surveillance policy and must not disclose, access or use information contained in the video surveillance system, its components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.";

(b) on page 6, under the heading "Unauthorized Access and/or Disclosure (Privacy Breach)", the last paragraph following the last bullet, be deleted and replaced with the following:

"A breach of this policy by an employee may result in discipline up to and including dismissal. A breach of this policy by service providers (contractors) to the City may result in termination of their contract.";

(c) in Appendix 3, delete the words "*City of Toronto Act, 1997* and the City of Toronto By-law 1120-2004", and replace with *"Municipal Act, 2001 and Occupiers' Liability Act*";

(d) in Appendix 6, at box 8B, delete the narrative contents and replace with the following:

"Understands that a breach of this policy by an employee may result in discipline up to and including dismissal. A breach of this policy by service providers (contractors) to the City may result in termination of their contract.";

(e) on page 3, under the heading "Designing and Installing Video Surveillance Equipment", delete the word "should" and replace it with the word "shall" where it appears in Bullet 2, 3 and 4 and delete the words "if possible" in Bullet 3 so that Bullets 2, 3 and 4 shall now read as follows:

"- The video equipment shall be installed to only monitor those spaces that have been identified as requiring video surveillance.

- Operators' ability to adjust cameras shall be restricted so that Operators cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program.

- Equipment shall never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms).";

(2) request the Chief Corporate Officer, in consultation with Union representatives, to develop a protocol to discuss and provide notice to Union representatives of the removal or addition of security video surveillance cameras;

(3) request all Agencies, Boards and Commissions to mirror in their by-laws the City of Toronto Security Video Surveillance Policy;

(4) request the Toronto Community Housing Corporation Board of Directors to consider adopting a policy on video surveillance at their properties; and

(5) request the Chief Corporate Officer to report back to the Administration Committee on the possibility of conducting a joint public meeting with the Toronto Police Service before the Toronto Police Services Board adopts a video surveillance policy.

The Administration Committee submits the report (May 15, 2006) from the Chief Corporate Officer.

Purpose:

To obtain Council approval of a policy on security video surveillance for City owned and leased properties.

Financial Implications and Impact Statement:

There are no immediate financial implications arising from this report. However, implementation of this policy may require the replacement of some existing security video surveillance cameras and recorders with updated video surveillance technology.

Recommendations:

It is recommended that Toronto City Council adopt the attached Security Video Surveillance Policy (Attachment 1) to this report.

Background:

This policy stems from a privacy investigation in response to a complaint lodged against the City of Toronto, made to the Information and Privacy Commissioner's Office/Ontario (IPC), in June 2003. The IPC complaint was based on concerns about the privacy implications associated with the use of surveillance cameras installed on the newly completed Yonge-Dundas Square.

In response to the privacy complaint, the Director, Corporate Access and Privacy worked directly with the Executive Director, Facilities and Real Estate and staff of Yonge-Dundas Square's Board of Management to address the various privacy concerns identified by the IPC regarding the collection, use, disclosure, retention and destruction of the personal information captured by the video surveillance cameras. As part of the privacy investigation of the IPC, the Director, Corporate Access and Privacy and the Executive Director, Facilities and Real Estate have worked with the IPC to develop a City-wide security video surveillance policy.

Institutions governed by the *Municipal Freedom of Information and Protection of Privacy Ac*t (MFIPPA) have statutory obligations imposed under Part II of the Act that govern the collection, use and disclosure of personal information. Therefore, where municipal institutions adopt the use of video surveillance cameras, the institutions have a duty to balance the security benefits derived from the use of video surveillance with the privacy rights of an individual to be free of unlawful collection, use and disclosure of their personal information. To this end, the IPC published a document entitled "Guidelines for Using Video Surveillance Cameras in Public Places". The intent of these IPC guidelines is to provide a framework to assist institutions when developing and implementing a video surveillance policy to ensure a lawful and justifiable policy choice that incorporates privacy protective measures and MFIPPA requirements into the system. Following the intent of the IPC guidelines, the City of Toronto Security Video Surveillance Policy has been drafted to ensure that information obtained through security video monitoring is used exclusively for security of City property purposes and released according to the standards set by MFIPPA.

An Interdivisional Working Group was established to develop a City-wide policy on video surveillance for security purposes and an inventory of existing City-owned installations of security video surveillance cameras. The working group, under the direction of the Manager, Security & Life Safety, Corporate Security, included representation from the Director, Corporate Access and Privacy, City divisions, and included feedback from some Agencies, Boards, and Commissions.

City of Toronto facilities, excluding facilities of ABCs, have approximately 734 security cameras at a total of 137 locations. Examples of the types of sites include: Civic Centres, Social Services facilities, Water facilities, Recreations Centres, etc.

In accordance with the IPC's guidelines, the City of Toronto's proposed Video Surveillance Policy was sent to the IPC for review and comment. On November 9, 2004, the IPC advised that it was pleased with the content of the Policy and commended the City on preparing a document that carefully addressed all the key requirements set out in the "Guidelines". The IPC however requested additional information on staff training and that a security threat assessment be provided. As a result of this request, two additional forms were forwarded to the IPC to satisfy their requirements: The City of Toronto Security Video Surveillance Policy Training Checklist and a Security Threat Assessment Form. On May 26, 2005, the City Clerk received a response from the IPC confirming that they received the two documents and were satisfied that they complied with the requirements set out in their Office's "Guidelines".

On June 28, 2005, the Administration Committee considered a Report (June 9, 2005) from the City Manager recommending that Toronto City Council adopt the submitted Security Video Surveillance Policy.

The Administration Committee referred the report back to the City Manager with a request for a revised policy. The policy was revised to require that Chief Corporate Officer report annually to the Administration Committee on all video surveillance and when video surveillance is being proposed for high-profile locations. A second revision changed the word "should" to "must" in the implementation guidelines.

On April 3, 2006 the City Clerk received further correspondence from the IPC inquiring on the status of the Security Video Surveillance Policy. A copy of the IPC correspondence is attached as appendix 3.

Comments:

Scope of Security Video Surveillance Policy (Attachment 1)

Attachment 1 is recommended to apply to all types of security camera surveillance systems, monitors and recording devices at City-owned and leased properties.

Attachment 1 is intended to encompass all types of camera surveillance for security purposes. The proposed policy provides a number of regulations to govern the use of video surveillance including:

(a) the designation of the Chief Corporate Officer of the City of Toronto as the responsible executive for the Security Video Surveillance Policy;

(b) identifying roles and responsibilities for personnel responsible for policy implementation and governance, as well as, individuals using and maintaining CCTV equipment;

(c) identifying factors to be considered prior to implementing video surveillance including: factors to consider prior to using cameras, considerations when designing and installing video surveillance equipment, providing notice of the use of video surveillance through posted signs, designating who and under what conditions personnel are authorized to operate camera equipment, and providing obligations to personnel who have access to records;

(d) addressing issues related to the collection, use, disclosure, retention and destruction of recordings in accordance with the privacy requirements of MFIPPA and its Regulations;

(e) detailing procedures to facilitate access to records, including formal access requests and access for law enforcement purposes; and,

(f) providing a review clause indicating that the policy will be reviewed every two years by the Chief Corporate Officer who will forward recommendations for update, if any, to City Council for approval.

Attachment 1 also contains a number of appendices, including: a Law Enforcement Officer Request Form; an Access / Correction Request form; a Notice of Collection sign; a document entitled “A Privacy Protocol: Guidelines for Managing a Privacy Breach”; a Surveillance Video Security Threat Assessment form; and a Video Surveillance Policy Training Checklist.

Response to Administration Committee recommendations

Consultation with the Unions:

Contained in the 2005 Memorandum of Agreement between the City and Union Local 416 is a Letter of Intent entitled "Video Security Surveillance; Global Positions Systems (GPS) and Automated Vehicle Location Systems". This Letter of Intent states that "The City will notify the Union when video security systems and GPS/AVL systems are used in the work location or fleets of vehicles where Local 416 employees regularly work. Uses for video security systems include the protection and safety of employees, members of the public, customers and City Assets and property…The City will consult with the Union within the first year of the Collective Agreement on the development of the policy with respect to Security Video Surveillance and a policy on GPS/AVL systems".

The City has consulted with union Local 416, Local 79 and Local 3888 (the Firefighter's Union) in the preparation of this policy. In response to consultation with the union representatives, a protocol will be established to provide notice to Union representatives of the removal or addition of security video surveillance cameras.

At the September 28-30, 2005 meeting of the Council of the City of Toronto, a notice of motion by Councillor Watson was carried that amended Administration Committee Report 7, Clause 15, headed "Corporate Access and Privacy (CAP) Office Renewal Update". This adopted clause stated "That staff bring a video surveillance policy report to the Administration Committee for discussion that addresses camera technology as it relates to compliance with privacy legislation; and City staff consult with staff of the Toronto Transit Commission and the Toronto Police Video services in this regard".

Attachment 1 was provided to the Toronto Police Services, Video Surveillance Unit for comment. The Toronto Police Services (TPS) advised the City Clerk's Office that the TPS has entered into a Closed Circuit Television (CCTV) proposal with the Ontario Ministry of Community Safety and Correctional Services to install video surveillance cameras in public spaces for the purposes of public safety.

The TPS is a recognized institution for the purposes of MFIPPA and, as such, has its own Access and Privacy Office. Although the TPS has not drafted a privacy policy on video surveillance, the Access and Privacy Offices of the City of Toronto and the TPS will actively collaborate on a policy that will incorporate the fundamental principles of City's Security Video Surveillance Policy and the IPC Guidelines. Legal staff at the Toronto Transit Commission have advised that they currently do not have a privacy policy on video surveillance but have been actively working on one.

Non-application of Policy:

Attachment 1 is not recommended to apply to "street" cameras or systems used to monitor buildings or properties not owned and managed by the City of Toronto. Any public safety policy regarding the prevention and enforcement of crime on public streets falls within the law enforcement mandate of the Police Service, not within a security mandate for City properties of the City of Toronto.

Attachment 1 does not apply to video surveillance used for employment related or labour-related information. The requirement for a Video Surveillance Policy is based upon the statutory obligations of MFIPPA. The *Municipal Freedom of Information and Protection of Privacy Ac*t does not apply to employment-related or labour-related information except for: 1. An agreement between an employer and a trade union; 2. A settlement agreement between an employer and one or more employees; 3. An agreement between an employer and one or more employees; and, 4. An expense account submitted by an employee to the employer.

Attachment 1 is not intended to apply to the RESCU Traffic Management cameras and red-light cameras used by the City. The Traffic Management Centre of the Transportation Services Division currently operates and monitors approximately 40 CCTV cameras located adjacent to the F.G. Gardiner Expressway, the Don Valley Parkway and Lake Shore Boulevard. The traffic management policy relates to the authority of Transportation Services to respond to roadway incidents that impact the safe and efficient operation of these roadways. The Ministry of Transportation cameras are on the 400 series highways and are the jurisdiction of the Province of Ontario. The Red Light Cameras are located at specific City intersections. These lights are governed by the 1998 amendment to the Highway Traffic Act (Bill 102, Chpt. 38 of Statutes of Ontario, 1998).

Attachment 1 in its current form is also not recommended to include Agencies, Boards, and Commissions (ABC's) of the City of Toronto; however, it is recommended that those ABCs that do not have a formal security video surveillance policy should adopt one as soon as possible.

Conclusions:

City Council adoption of the Security Video Surveillance Policy, appended to this report, would directly address and conclude the IPC investigation of the 2003 Yonge-Dundas privacy complaint against the City and allow the City to be compliant with privacy legislation. Further, this policy would create an administrative framework for all current and future proposed video use at City owned and leased properties to ensure compliance with MFIPPA.

Contacts:

Chuck Donohue, P. Eng.
Executive Director, Facilities & Real Estate
Telephone: 416-397-5151
E-mail: cdonohue@toronto.ca

Suzanne Craig
Director, Corporate Access and Privacy
Telephone: 416-392-9683
E-mail: scraig@toronto.ca

Security Video Surveillance Policy

Policy Statement

The City of Toronto (the City) recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of City employees, clients, visitors and property. While video surveillance cameras are installed for safety and security reasons, the

City's video surveillance systems must also be designed to minimize privacy intrusion. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep City facilities and properties operating in a safe, secure, and privacy protective manner.

Policy Description

This City policy has been developed to govern video surveillance at City owned and leased properties in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Application

This policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices at City owned and leased properties that are used for security purposes.

This policy does not apply to the RESCU Traffic Management and Red Light cameras used in the City; the City's Agencies, Boards, and Commissions; cameras used by the Toronto Police Service; or, to video surveillance used for employment related or labour-related information.

Responsibilities

The senior staff member responsible for the Video Surveillance Policy is the Chief Corporate Officer.

Roles and Responsibilities

Responsibilities of Chief Corporate Officer

The Chief Corporate Officer may delegate various responsibilities under this Policy to Division Heads. The key duties of the Chief Corporate Officer include:

- Ensuring City-wide Policy compliance.
- Undertaking yearly evaluations of video surveillance system installations to ensure compliance with the City's Security Video Surveillance Policy.
- Reviewing the Policy every 2 (two) years and forwarding recommendations for update, if any, to City Council for approval.
- Receiving status updates from the Executive Director, Facilities and Real Estate, every six months, regarding staff adherence to the responsibilities within the policy.
- Reporting to the Administration Committee when video surveillance is being proposed for high profile locations (i.e. locations with a high number of members of the public) and on annual basis on all security video surveillance equipment installed.

Responsibilities of Manager, Security and Life Safety, Corporate Security

As designated by the Executive Director, Facilities & Real Estate, the Manager, Security & Life Safety shall:

- Conduct Security Threat Assessments to determine the requirement for a video surveillance system.
- Prepare recommendations for the Executive Director, Facilities & Real Estate for review and installation approval of video surveillance systems.
- Approve installation of video cameras at specified City owned and leased properties.
- Advise on placement of video surveillance monitoring signs.
- Delegate day-to-day operations of video systems to Designated Divisional Management staff (DDM).
- Conduct periodic internal audits to ensure compliance with the Security Video Surveillance Policy.
- Act as a designate contact for all requests by law enforcement agencies for access to video records.
- In consultation with the Director, Corporate Access and Privacy, develop privacy training for City and contract staff that have responsibilities under this Policy.
- Immediately report all alleged privacy breaches to the Director, Corporate Access and Privacy for immediate action.

Responsibilities of Designated Divisional Management Staff (DDM)

Designated Divisional Management staff (DDM) are appointed by their respective Division Head to be responsible for the video operations at their site location(s). The responsibilities of a Designated Divisional Management staff member include:

- Overseeing day-to-day operations of video surveillance cameras at their workplace.
- Providing supervision to approved Operators.
- Complying and ensuring Operator's compliance with all aspects of the Security Video Surveillance Policy.
- Ensuring monitoring and recording devices are stored in a safe and secure location.
- Ensuring logbooks, recording all activities related to video devices and records, are kept and maintained by operators.
- In consultation with the Director, Corporate Access and Privacy, providing training on a regular basis to Operators regarding obligations and compliance with the MFIPPA and the Security Video Surveillance Policy.

Responsibilities of Operators

Operators are City staff or contracted individuals entrusted by a Designated Divisional Management staff member to operate the video surveillance system for a particular facility. The duties and responsibilities of the Operator include:

- Complying and adhering to all aspects of the Video Surveillance Policy.

- Monitoring the video surveillance cameras.
- Ensuring all aspects of the video surveillance system are functioning properly.
- Documenting all information regarding the use, maintenance, and storage of records in the applicable logbook, including all instances of access to, and use of, recorded material to enable a proper audit trail.
- Ensuring that no personal information is disclosed without the approval of the Manager, Security and Life Safety.
- Ensuring that no copies of data/images in any format (hardcopy, electronic, etc.) is taken from the video surveillance system without approval from the Manager, Security and Life Safety.
- Forwarding all requests for access to video records to the Manager, Security and Life Safety, Corporate Security. The Manager, Security and Life Safety, Corporate Security will consult with the Director, Corporate Access and Privacy and / or forward requests / complaints to the Director, Corporate Access and Privacy for processing.

Responsibilities of the Director, Corporate Access and Privacy

The key duties of the Director, Corporate Access and Privacy in relation to this Policy include:

- Providing advice and recommendations to divisional staff to assist in compliance with the MFIPPA.
- Processing access requests for video surveillance records.
- Responding to privacy complaints related to video installations.
- Investigating video surveillance security / privacy breaches.
- In consultation with Designated Divisional Management staff, providing training on a regular basis to Operators regarding obligations and compliance with the MFIPPA and the Security Video Surveillance Policy (See Appendix #6: Video Surveillance Policy Checklist).

Responsibilities of All City Staff

All City Staff must adhere to the video surveillance policy and must not access or use information contained in the video surveillance system, it's components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.

Guidelines to Follow Prior to the Implementation of a Video Surveillance System

Factors to Consider Prior to Using Video

Before deciding to install video surveillance, the following factors must be considered:

- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- An assessment must be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated.
- The proposed design and operation of the video surveillance systems should minimize privacy intrusion.

A form has been provided to assist in reviewing these factors. (See Appendix #5: Surveillance Video Security Threat Assessment)

Designing and Installing Video Surveillance Equipment

When designing a video surveillance system and installing equipment, the following must be considered:

- Given the open and public nature of the City's facilities and the need to provide for the safety and security of employees and clients who may be present at all hours of the day, the City's video surveillance systems may operate at any time in a 24 hour period.
- The video equipment should be installed to only monitor those spaces that have been identified as requiring video surveillance.
- Operators' ability to adjust cameras should be restricted, if possible, so that Operators cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program.
- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms).
- Where possible, video surveillance should be restricting to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.
- Reception/recording equipment must be located in a strictly controlled access area. Only Designated Divisional Management staff, or those properly authorized in writing by the DDM, shall have access to the controlled access area and the reception/recording equipment.
- Every reasonable attempt should be made by video Operators to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

Notice of Use of Video Systems	In order to provide notice to individuals that video is in use: - The City shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under video surveillance. - The notification requirements of this sign must inform individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection. (See Appendix #3 – Notice of Collection)
Personnel Authorized to Operate Video Equipment	Only employees (Operators) and contractors designated by the Manager, Security and Life Safety, Corporate Security, or the DDM, shall be permitted to operate video surveillance systems.

Video Equipment / Records

Types of Recording Devices	The City may use either Digital Video Recorders (DVR) or time lapse Video Cassette Recorders (VCR's) in its video systems. Facilities using video recorders will retain these records for a period of 30-60 days depending on the recording device and technology. A record of an incident will only be stored longer than the 30-60 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes.
Record Identification	All records (storage devices) shall be clearly identified (labelled) as to the date and location of origin including being labelled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a harddrive, the computer time and date stamp shall be understood to be this identification. In facilities with a VCR or other recording mechanism using a removable / portable storage device, the operator shall affix a label to each storage device identifying this information.
Logbook	Each Operator shall maintain a logbook to record all activities related to video devices and records. The activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All logbook entries will detail authorized staff, date, time and activity. This logbook must remain in a safe and secure location with the video recording equipment. Only the DDM or Manager, Security & Life Safety are authorized to remove this logbook from the secure location.

Access to Video Records

Access	Access to the video surveillance records, e.g. logbook entries, CD, video tapes, etc shall be restricted to authorized personnel only to in order to comply with their roles and responsibilities as outlined in the Video Surveillance Policy.
Storage	All tapes or other storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.
Formal Access Requests Process	With exception of requests by law enforcement agencies, all requests for video records should be directed to the Corporate Access and Privacy office for processing. A person requesting access to a record should make a request in writing either in the form of a letter or the prescribed form (See Appendix #2: Access / Correction Form) and submit it to the Director, Corporate Access and Privacy. The individual requesting the record must: - Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an experienced employee of the City of Toronto, upon a reasonable effort, to identify the record; and, - At the time of making the request, pay the prescribed fees as provided for under the Act.
Access: Law Enforcement	If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the City's Law Enforcement Officer Request Form (See Appendix #1) and forward this form to the Manager, Security & Life Safety, Corporate Security or designate. The Manager, Security & Life Safety, or designate, will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer. The Manager, Security & Life Safety, Corporate Security, or designate, will record the following information in the facility's video logbook: i) the date and time of the original, recorded incident including the designated name/number of the applicable camera and VCR/DVR; ii) the name of the Operator at the time of the incident; iii) the time and date the copy of the original record was sealed; iv) the time and date the sealed record was provided to the requesting Officer; and, v) if the record will be returned or destroyed after use by the Law Enforcement Agency.

Viewing Images	When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be completed by an individual(s) authorized by the DDM in a private, controlled area that is not accessible to other staff and/or visitors.
Custody, Control, Retention and Disposal of Video Records / Recordings	The City of Toronto retains custody and control of all original video records not provided to law enforcement. Video records are subject to the access and privacy requirements of the MFIPPA, which includes but is not limited to the prohibition of all City Staff from access or use of information from the video surveillance system, it's components, files, or database for personal reasons. With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, the City must not maintain a copy of recordings for longer than the recording systems' 30-60 day recording cycle. The City will take all reasonable efforts to ensure the security of records in its control / custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.
Unauthorized Access and/or Disclosure (Privacy Breach)	City staff who become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Manager, Security and Life Safety and the 4Director, Corporate Access and Privacy. After this unauthorized disclosure or potential privacy breach is reported: - Upon confirmation of the existence of a privacy breach, the Director, Corporate Access and Privacy shall notify the Information and Privacy Officer of Ontario (IPC) and work constructively with the IPC staff to mitigate the extent of the privacy breach and to review the adequacy of privacy protection with the existing policy. - The Manager, Security and Life Safety, Corporate Security shall inform the Director, Corporate Access and Privacy of events that have led up to the privacy breach (See Appendix 4: Privacy Protocol: Guidelines for Managing a Privacy Breach). - The staff member shall work with the Manager, Security and Life Safety, Corporate Security and the Director, Corporate Access and Privacy to take all reasonable actions to recover the record and limit the record's disclosure.

- The Director, Corporate Access and Privacy, in consultation with the Manager, Security and Life Safety, and where required, will notify affected parties whose personal information was inappropriately disclosed.

- The Director, Corporate Access and Privacy, in consultation with the Manager, Security and Life Safety shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

Intentional wrongful disclosure, or disclosure caused by negligence, by employees of the City may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by service providers (contractors) to the City, may result in termination of their contract.

Inquires From the Public Related to the Video Surveillance Policy	A staff member receiving an inquiry from the public regarding the Video Surveillance Policy shall direct the inquiry to the Manager, Security & Life Safety, Corporate Security at 416-397-0000.
Review of Video Surveillance Policy	This policy shall be reviewed every 2 (two) years by the Chief Corporate Officer who will forward recommendations for update, if any, to City Council for approval.
Approved by	
Date Approved	

_____

Appendix 1 - Law Enforcement Officer Request Form

RELEASE OF RECORD TO LAW ENFORCEMENT AGENCY
UNDER SECTION 32(G) OF THE
MUNICIPAL FREEDOM OF INFORMATION AND
PROTECTION OF PRIVACY ACT

TO: City of Toronto _____ Division

I, _____, of the _____
Print Name of Police Officer Print Name of Police Force

request a copy of the following record(s):

1.

2.

3.

containing the personal information of _____
Print Name(s) of Individual(s)

to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

_____	_____	_____
Signature of Officer	Badge/Identification No.	Date

_____	_____
Print Name of Manager, Security & Life Safety or Designate Releasing Recording	Signature of Manager, Security & Life Safety or Designate Releasing Recording

Return all completed ORIGINAL forms to the Corporate Access and Privacy Office, City Clerk's Office, City Hall, 13th Floor, 100 Queen Street West, Toronto, Ontario, M5H 2N2. Should you have any questions regarding the use of this form, please contact the Director, Corporate Access and Privacy at (416) 392-9683.

Appendix 2 – Access/Correction Request

Municipal Freedom of Information and Protection of Privacy Act/Personal Health Information Protection Act

Application Fee *$5.00**.*** An application fee of $5.00 is to accompany all requests for information and/or correction requests. Please make cheque/money order payable to City of Toronto. Forward to the Corporate Access and Privacy Office at 13th Floor West Tower, City Hall, 100 Queen Street West, Toronto, ON M5H 2N2.

Please include a copy of a signed form of identification, with any request for your own personal or personal health information.

Request for:

☐ Access to General Records

☐ Access to Own Personal Information/Personal Health Information

☐ Correction of Own Personal Information/ Personal Health Information

City of Toronto
Identify Dept.: .....

.....

Other Institution: .....

(If applicable)

Last Name	First Name	Initial	Daytime Telephone No. ( )

Address	Suite	City/Town	Prov.	Postal Code	Evening Telephone No ( )

Detailed description of requested records, personal information records or personal information to be corrected.

** If you are requesting a correction of personal information, please indicate the desired correction and attach any supporting documentation.

Preferred method of access to records: ☐ Examine Original Or ☐ Receive Copy

* Fees: Please note processing costs (i.e., photocopying, postage) may apply. See Fee Schedule on back of application form.

Signature Of Applicant Date

Day Month Year

Office Use Only

☐ MFIPPA ☐ PHIPA ☐ BOTH

Date Request Received	Date Application Fee Received	Date Due	Request Number
Day Month Year	Day Month Year	Day Month Year	

Personal information contained on this form is collected pursuant to the Municipal Freedom of Information and Protection of Privacy Act, and will be used for the purpose of responding to your request. Questions about this collection should be directed to the Director, Corporate Access and Privacy Office, at (416) 392-9683.

Summary of Fees

A: For Information Requests Under the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*

The rules regarding the payment and amount of fees are set out in the *Act* and its regulations. The fees that are permitted are:

Fees for Requests for Personal Information

A request for information about oneself is considered a "personal information request".

The following fees apply to requests for your own personal information:

Application Fee:	$5.00 - To be paid when you submit your request; Application Fee is mandatory and not subject to waiver
* Photocopying:	$0.20 / page (Requester's copy only)
Computer Programming:	$15.00 per ¼ hour if needed to develop program to retrieve information;
Diskettes/CD's:	$10.00 for each diskette/CD

Fees for Requests for General Information

Requests for information, whether about a person other than yourself or about a government program or activity are considered "general information requests".

The following fees apply to a request for general information:

Application Fee:	$5.00 - To be paid when you submit your request; Application Fee is mandatory and not subject to waiver
Search Time:	$7.50 per ¼ hour required to search and retrieve records;
Record Preparation (i.e. severing):	$7.50 per ¼ hour required to prepare records for release;
* Photocopying:	$0.20 / page (Requester's copy only)
Computer Programming:	$15.00 per ¼ hour if needed to develop program to retrieve information;
Diskettes/CD's:	$10.00 for each diskette/CD

* Please note that the individual will be provided the option of viewing originals on site. Select photocopying fees may apply.

B: For Information Requests Under the *Personal Health Information Protection Act* (*PHIPA*)

Same fees are applicable as for requests for personal information under *MFIPPA.*

_____

Appendix 3
Notice of Collection

Appendix 4 - Privacy Protocol: Guidelines for Managing a Privacy Breach

Introduction

What is a privacy breach?

A privacy breach occurs when personal information is collected, used, disclosed and/or destroyed in ways that are not in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

The most common breach of personal information is the unauthorized disclosure of personal information contrary to section 32 of the *Act.* Types of breaches include a lost or misplaced file, a lost or stolen laptop, unauthorized access to personal information (electronic/hardcopy) or the inadvertent disclosure of personal information (e.g. human error in misdirecting a fax or e-mail).

When faced with a potential privacy breach, take the following actions immediately:

Identify the scope of the potential breach and take steps to contain it

- Ensure appropriate staff within the City are immediately notified of the breach, including the Director, Corporate Access and Privacy office (CAP) at 392-9683, the City Clerk, and the appropriate Division Head and Deputy City Manager.

- Immediately isolate any physical or system resource that may contain evidence (e.g., paper files, workstations, logs, electronic records, e-mail files, etc.)

- Keep existing back-ups (take tapes out of circulation) and back up any system resource associated with the incident.

- Retrieve the hard copies of any personal information disclosed.

- Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required.

- In consultation with the appropriate staff, determine whether the privacy breach could allow unauthorized access to any other personal information.

- Document all actions (dates and times) taken during containment.

- Determine if the response to the incident needs to be escalated (e.g., to a law enforcement agency).

Notify the affected individual(s) of a privacy breach:

- Identify those individuals whose privacy was breached and, barring exceptional circumstances (e.g. no known last address), notify those individuals (e.g., by telephone or in writing).

- Provide details of the extent of the breach and the specifics of the personal information at issue and advise of the steps that have been taken to address the breach, both immediate and long-term.

Investigate the privacy breach

- CAP will inform the Information and Privacy Commissioner/Ontario (IPC/O) Registrar of the privacy breach and advise of immediate containment and notification actions taken by the City department.

- CAP, in consultation with the IPC and department staff will conduct an internal investigation into the matter. The objectives of the investigation are to ensure the immediate requirements of containment and notification have been addressed; review the circumstances surrounding the breach; review the adequacy of existing policies and procedures in protecting personal information and implement changes to prevent future breaches. Program-wide or institution-wide procedures may warrant a review, (incidents such as a misdirected fax transmission; or inadequate system access controls).

- CAP will advise the IPC in writing of our findings and work together with department staff and the IPC to make any necessary changes. The IPC may issue a report with recommendations.

Resolution/Remedies

- Implement IPC recommendations (e.g., revising and or developing policies, procedures).

- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the *Act.*

Conclusion

These guidelines have been prepared by the Corporate Access and Privacy office and are intended to provide basic information on how to proceed in the event of a privacy breach.
For more information about the guideline, please contact the Manager, Training and Compliance, Corporate Access and Privacy at 392-9674.

_____

Appendix 5
Surveillance Video Security Threat Assessment
To Determine the Requirements for a Video Surveillance System

Site Name: _____ Location: _____Requestor: _____ Division: _____

Date: _____ Video # _____ Proposed Video Location: _____

1. Is there already a video surveillance system and/or camera on site? If so. Please describe and advise if their set-up adheres to the City of Toronto's Security Video Surveillance Policy? (Use separate page if required)

2. Video surveillance should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Have the following security counter-measures been considered and rejected as unworkable?

#2	Security Counter-Measure	Yes	No	Comments
A	Security Procedures			
B	Duress Buttons			
C	Door Locking Hardware			
D	Alarm System			
E	Access Control System			
F	Signage			
G	Security Guard/Officer Patrols			
H	Lighting			
I	Other: (CPTED, etc)			

3. The use of each video surveillance camera should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns. Are there any documented incidents of crime or significant safety concerns in any of the following formats?

#3	Documentation Formats	Yes	No	Comments
A	Corporate Security Occurrence Reports			
B	Police Reports			
C	H&S Consultants Report			
D	H&S Committee Minutes			
E	Internal Memos			
F	Other:			

4. An assessment should be conducted on the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects can be mitigated. Has the following effects and mitigation strategies been considered?

#4	Effects & Mitigation Strategies	Yes	No	Comments
A	The location of the proposed camera is situated in an area that will minimize privacy intrusion?			

#4	Effects & Mitigation Strategies	Yes	No	Comments
B	Is the proposed camera location one where the public and employees do not have a higher expectation of privacy (i.e. not in a washroom or change room, etc)?			
C	Is the location of the proposed video camera visible?			
D	Can the video surveillance be restricted to the recognized problem area?			
E	Is space allocated for proper video surveillance signage?			
F	Has a drawing been attached showing the video location?			
G	Other:			

5. The proposed design and operation of the video surveillance systems should minimize privacy intrusion. Have the following design and operation factors been considered for each proposed camera location?

#5	Measures to Mitigate Effects	Yes	No	Comments
A	Can the proposed camera be restricted through hardware or software to ensure that Operators cannot adjust or manipulate cameras to overlook spaces that a threat assessment has not been completed for?			
B	Is the reception equipment going to be located in a strictly controlled access area?			
C	Can the Video Surveillance Monitor be installed in such as way that it will be hidden from public view?			
D	Other:			

Comments:

_____ _____ _____ _____

Completed By (Print) Signature Date
Position Title

Appendix 6

Security Video Surveillance Policy Training Checklist

Employee or Service Providers Name:
Division / Section or Company:
Position Title:

General Statement

The Information and Privacy Commissioner of Ontario published "Guidelines for Video Surveillance Cameras in Public Places" that forms the basis of the City of Toronto's Video Surveillance Policy. These guidelines state that a Video Surveillance Policy should include "…the incorporation of the policy into training and orientation programs of an institution and service provider" and that these "…training programs addressing staff obligations under the act should be conducted on a regular basis".

The City of Toronto intends to meet these obligations through the use of this Training Checklist and formal training completed in consultation with Corporate Security and the Corporate and Privacy Office (CAP) on a regular basis.

1. Policies and Procedures

#	Question	Yes	No	Comments
A	Has received a copy of, read and understood the City of Toronto's Security Video Surveillance Policy?			
B	Has received a copy of, read and understood the applicable appendices to the City of Toronto's Video Surveillance Policy?			
C	Has received a copy of, read and understood the document entitled: Privacy Protocol: Guidelines for Managing a Privacy Breach?			

2. Roles and Responsibilities

#	Question	Yes	No	Comments
A	Understands the roles and responsibilities of the Chief Corporate Officer; the Manager, Security and Life Safety; the Designated Divisional Management staff, CCTV Operators, the Corporate Access and Privacy Office; and all City staff?			
B	Understands and will carry out the duties and responsibilities of the Operator?			

3. Guidelines for the Implementation of a Video Surveillance System

#	Question	Yes	No	Comments
A	Is aware that video surveillance equipment should only be installed and used to monitor those spaces that have been identified as requiring video surveillance?			
B	Is aware that no person shall adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program?			
C	Is aware that equipment should never be used to monitor the inside of areas where the public and employees have a higher expectation of privacy? (i.e. washrooms, change rooms, etc.)			
D	Is aware that all video surveillance installations must be clearly marked to advise staff and members of the public that video surveillance is in use?			
E	Is aware that signs shall be posted at all entrances and/or on the perimeter of the grounds under video surveillance?			

4. Video Surveillance Equipment / Records

#	Question	Yes	No	Comments
A	Has read, understood, and will follow the requirements for Record Identification, as stated in the City of Toronto's Security Video Surveillance Policy?			
B	Is aware that each Video Surveillance Operator shall maintain a logbook to record all activities related to video surveillance devices and records and that each entry will detail authorized staff, date, time, and activity?			
C	Is aware that Video Surveillance Operators must document all information regarding the use, maintenance, and storage of records in the logbook, including all instances of access to, and use of, recorded material to enable a proper audit trail?			
D	Is aware that Video Surveillance Operators may not deliberately enter false or incomplete information or delete existing information in any logbook and may not take any unauthorized action that would cause the destruction or alteration of any information contained in any logbook?			
E	Is aware that Video Surveillance Operators shall not make any changes to the identification or labels of records either in hardcopy or computerized formats?			
F	Is aware all tapes or other storage devices that are not in use must be securely stored in a locked receptacle located in an access-controlled area?			
G	Is aware that Video Surveillance Operators shall not make any copies of data/images in any format (hardcopy, electronic, etc) from the video surveillance system without approval from the Manager, Security & Life Safety, Corporate Security, following the protocols set out in the Video Surveillance policy?			

5. Access to Video Surveillance Records

#	Question	Yes	No	Comments
A	Is aware that Video Surveillance Operators may access information only when necessary to perform work assigned by a Designated Divisional Management Staff member to accomplish the City's mission and objectives?			
B	Is aware that Video Surveillance Operators must not access or use information from any component(s) of the Video Surveillance system files or database for personal reasons?			
C	Is aware that access to the video surveillance records e.g. logbook entries, CD's, videotapes, etc. shall be restricted to authorized personnel only?			
D	Is aware that the Video Surveillance Operator shall not disclose personal information and that disclosure should only occur by the Designated Divisional Management Staff member in consultation, as necessary, with the Corporate Access and Privacy Office to ensure that information is being disclosed in accordance with the *Municipal Freedom of Information & Protection of Privacy Act?*			
E	Is aware of and understands the Formal Access Request process and the use of the "Access / Correction Form"?			
F	Is aware of and understands the Formal Access Request process for Law Enforcement Personnel and the use of the "Law Enforcement Officer Request Form"?			

6. Viewing Images

#	Question	Yes	No	Comments
A	Understands that video surveillance monitors should be concealed as much as possible from the general public and unathorized employees?			
B	Understands when recorded images from the camera must be viewed (for law enforcement or investigative reasons) this must occur in a private, controlled area that is not accessible to other staff and/or visitors.			

7. Retention and Disposal of Records

#	Question	Yes	No	Comments
A	Is aware that a Video Surveillance Operator must not dispose, destroy, or erase any record without proper authorization and without following the regulations contained in the Video Surveillance Policy?			
B	Is aware that with the exception of requests by Law Enforcement agencies for copies of video surveillance recordings specific to a reported incident / investigation, the City does not maintain a copy of recordings provided in response to a law enforcement request?			
C	Understands that video surveillance records will only be retained for a 30 to 60 day period depending upon the type of technology for non-incident recording.			
D	Understands that the Video Surveillance Operator shall take all reasonable efforts to ensure the security of records in the City's custody and control?			
E	Understands that all storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased, shredded, or burned and cannot be retrieved or reconstructed?			

8. Unauthorized Access and/or Disclosure

#	Question	Yes	No	Comments
A	Understands that any Video Surveillance Operator and/or any City staff who become aware of any unauthorized disclosure of a video surveillance record in contravention of the City of Toronto's Video Surveillance Policy and/or a potential privacy breach are to immediately notify the Manager, Security and Life Safety and the CAP Office?			
B	Understands that intentional wrongful disclosure, or disclosure caused by negligence, by employees of the City may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by service providers (contractors) to the City, may result in termination of their contract?			

9. Inquiries from the Public

#	Question	Yes	No	Comments
A	Is aware that any Video Surveillance Operator receiving an inquiry from the public regarding the Security Video Surveillance Policy shall direct the inquiry to the Manager, Security & Life Safety, Corporate Security, at 416-397-0000?			

10. Audit

#	Question	Yes	No	Comments
A	Is aware that the Manager, Security & Life Safety, Corporate Security will designate staff to conduct random site visits or audits to ensure the Video Surveillance Policy is being followed?			

Print Name of Employee / Provider	Signature of Employee / Provider	Date
Witnessed by (Print) DDM	Signature of DDM	Date

The Administration Committee considered a communication (June 5, 2006) from Ann Dembinski, President, Local 79, Canadian Union of Public Employees.

Deputy Chief Tony Warr, Toronto Police Services, was present to respond to questions.