17.

STAFF REPORT
ACTION REQUIRED

Security Video Surveillance Policy – Revisions

Date:	September 24, 2018
To:	Toronto Public Library Board
From:	City Librarian

SUMMARY

The purpose of this report is to request the Toronto Public Library (TPL) Board's approval of revisions to the Security Video Surveillance Policy. The Security Video Surveillance Policy was first adopted by the Board at its March 26, 2007 meeting.

The key updates to the policy include:

- a revised Policy Objective which explains TPL's process for installation and use of security video surveillance equipment;
- adoption of an evidence-based approach to installation of surveillance camera equipment in relation to TPL properties, including the use of a needs assessment form;
- balancing the need to maintain a safe and welcoming environment while protecting the personal privacy of customers, staff, and service providers; and
- accountabilities in relation to surveillance camera installation approval, privacy, access requests, and legislative compliance.

RECOMMENDATIONS

The City Librarian recommends that the Toronto Public Library Board:

1. approves the revised Security Video Surveillance Policy in Attachment 1;

2. receives the revised Security Video Surveillance General Procedures for information in Attachment 2;

3. receives the Process for Acquiring Security Camera Equipment document for information in Attachment 3; and

4. receives the TPL Security Video Surveillance System Needs Assessment Form for information in Attachment 4.

FINANCIAL IMPACT

The recommendations in this report have no financial impact beyond what has already been approved in the current year's budget.

The Director, Finance & Treasurer has reviewed this financial impact statement and agrees with it.

DECISION HISTORY

At its March 26, 2007 meeting, the Toronto Public Library Board approved the addition of a Security Video Surveillance Policy (source: https://www.torontopubliclibrary.ca/about-the-library/board/meetings/2007-mar-26.jsp).

ISSUE BACKGROUND

Toronto Public Library recognizes the need to balance individual privacy rights against the broader need for community safety and security for TPL employees, staff and service providers. Security video surveillance is an integral component of TPL's security framework. Recording surveillance footage allows the Library to monitor the integrity of capital assets while maintaining public safety and assisting law enforcement in the investigation of suspected unlawful activity.

The TPL Security Video Surveillance Policy has been developed to govern security video surveillance of public areas, access, and disclosure in accordance with the Municipal Freedom of Information and Protection of Privacy Act and references the latest guidelines for surveillance in public areas as indicated by the Information and Privacy Commissioner of Ontario (IPC).

The deployment of security video surveillance systems within the TPL system is governed by the doctrine of minimal intrusion. While surveillance systems collect personal information, it is the sensitivity of that information that informs whether or not the benefits of surveillance outweigh the reduction in personal privacy of the individual.

Toronto Public Library considers two main factors when deciding to deploy security video surveillance: 1) the nature of the space under observation; and 2) the closeness of surveillance. These considerations (as well as related concepts) are documented in the "Process for Acquiring Security Camera Equipment" and "TPL Security Video Surveillance System Needs Assessment Form", Attachments 3 and 4, respectively. TPL processes also require documented, verifiable accounts of the need for a surveillance camera system in a particular area before deciding whether or not to deploy a new camera. The use of a Privacy Impact Assessment for the security video surveillance system provides further accountability for TPL's surveillance camera deployment process. Further information regarding TPL's security video surveillance system deployment considerations are documented in Attachments 3 and 4 of this report.

COMMENTS

The revised Security Video Surveillance Policy is implemented through the Security Video Surveillance General Procedures that are included in this report for information as Attachment 2. The revisions to the procedures include a simplified list of TPL staff that are authorized to access security video surveillance imagery for one of the following reasons:

a) Providing security video surveillance images to law enforcement agencies for law enforcement proceedings;
b) Investigating health & safety, security, or other incidents not requiring the involvement of law enforcement agencies, in consultation with management staff; and
c) Providing technical troubleshooting support.

The procedure further details the decision-making process surrounding camera installation and removal, demonstrating a consultative approach involving TPL Senior Management.

CONTACT

Elizabeth Glass; Director, Policy, Planning, and Performance Management;
Tel.: 416-395-5602; Email: eglass@torontopubliclibrary.ca

Paul Trumphour; Director, Transformational Projects; Tel.: 416-629-6598;
Email: ptrumphour@torontopubliclibrary.ca

Moe Hosseini-Ara; Director, Branch Operations and Customer Experience;
Tel.: 416-397-5944; Email: mhoss@torontopubliclibrary.ca

SIGNATURE

_____

Vickery Bowles
City Librarian

ATTACHMENTS

Attachment 1: Security Video Surveillance Policy
Attachment 2: Security Video Surveillance General Procedures
Attachment 3: Process for Acquiring Security Camera Equipment
Attachment 4: TPL Security Video Surveillance System Needs Assessment Form
Attachment 5 Comparison Document concerning revisions to Security Video Surveillance Policy (clean copy)
Attachment 6: Comparison Document concerning revisions to Security Video Surveillance General Procedures (clean copy)

Attachment 1

POLICY: **SECURITY VIDEO SURVEILLANCE**

SECTION: **Section V – Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56**

MOTION#/DATE: **07 - 057 – March 26, 2007**
18 - xxx – September 24, 2018

Effective Date

~~March 26, 2007~~September 24, 2018

Table of Contents

DRAFT

DRAFT

Policy Objective

The purpose of the Video Surveillance Policy is to describe Toronto Public Library's installation and use of video surveillance equipment in the interests of privacy, public safety, protection of property, and to maintain a safe and welcoming environment for library customers, staff, and service providers. ~~To ensure that, in adopting the use of security video surveillance cameras, Toronto Public Library balances the security benefits derived from the use of video surveillance with the privacy rights of the individual.~~

Underlying Principles

Underlying the Policy Objective is Toronto Public Library's commitment to maintaining a safe and welcoming environment for staff and members of the public. Toronto Public Library will achieve this through a modern, cohesive security system that strives to minimize intrusions upon the personal privacy of customers, staff, and service providers. Video surveillance is to be deployed on the basis of a formal needs-assessment carried out by designated Toronto Public Library staff. Through the use of a prescribed protocol, designated staff will be empowered to determine how video surveillance equipment will be deployed based on Toronto Public Library's security needs. Video surveillance will only be deployed for identifiable purposes that are consistent with this Policy. ~~In the daily operation of Toronto Public Library (TPL) premises, the safety of property, visitors, and employees is protected and maintained by conventional means such as: alert observation by staff, foot patrols by security personnel, security-conscious design of Library locations, safe behaviour training, and the consistent application of the Library's Rules of Conduct. However, in some circumstances, the additional protection provided by surveillance cameras is essential in maintaining lawful and safe use of Library premises.~~

The Security Video Surveillance Policy provides detailed direction concerning the context, procedures, and protocols within which the Library installs and operates surveillance cameras. The Policy ensures that the Library follows the guidelines set out by the ~~Ontario~~ Information and Privacy Commissioner of Ontario~~/Ontario,~~ and the privacy requirements of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), without compromising the safety and security of Library visitors, staff, and premises.

DRAFT

Policy Statement

This Policy is in place to maintain public safety and security of property through adequate monitoring of library facilities. The deployment of surveillance cameras and monitoring systems is achieved through the consistent use of an evidence-based approach to camera deployment. This protocol is detailed under the "Specific Directives" section of this Policy. Video surveillance deployment is guided by the principle of minimal intrusion by video surveillance systems into the daily operation of library facilities. Video surveillance systems are deployed only when needed based on criteria established within the Specific Directives. Library premises are monitored in the interest of asset protection, and to maintain safe library premises that are welcoming to library staff and visitors. ~~Toronto Public Library recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of Library employees, clients, visitors and property. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep Library facilities and properties operating in a safe and secure manner. While video surveillance cameras are installed for safety and security reasons, the Library's video surveillance systems must be designed and maintained to minimize privacy intrusion.~~

Scope

This Policy applies to all ~~types of~~ surveillance camera ~~surveillance~~ systems, ~~surveillance~~ deployed across all Library-owned and/or leased properties. This Policy does not apply to video surveillance used for employment-related or labour-related information.

Application

This Policy applies to ~~the~~ all Toronto Public Library staff and contracted workers. ~~Library contractors and service providers who have responsibilities relating to security video surveillance~~ All parties will be made aware of this Policy, their obligation to comply with it, and given instructions in meeting the Policy's requirements.

Specific Directives

A. Protocol for Implementation of a Video Surveillance System at a particular site: ~~Guidelines to Follow Prior to the Implementation of a Video Surveillance System~~ Factors to Consider Prior to Using Video

DRAFT

The Toronto Public Library has developed a needs based assessment process for acquisition and installation of a surveillance camera. The documents developed in relation to this are:

A. TPL Security Video Surveillance System Needs Assessment Form;
B. Process for Acquiring Security Camera Equipment

1. Factors to Consider Prior to Using Video

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

(a) The number of verifiable incidents of crime or significant safety concern; ~~The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns~~;
(b) The level of risk to the safety of staff and customers posed by such incidents;
(c) the potential for violation of the Library's Rules of Conduct;
(d) A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable;
(e) On a system-wide basis, ~~A~~ a Privacy Impact Assessment (PIA) must be conducted on the effects that the proposed video surveillance may have on personal privacy. The PIA should indicate mitigation strategies to limit adverse effects relating to privacy; and ~~the ways in which any adverse effects can be mitigated;~~
(f) The proposed design and operation of the video surveillance systems should minimize privacy intrusion.

1. Designing and Installing Video Surveillance Equipment

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

(a) Given the open and public nature of the Library's facilities and property, and the need to provide for the safety and security of individuals who

DRAFT

may be present at all hours of the day, the Library's video surveillance systems may operate at any time in a 24-hour period;

(b) The video equipment shall be installed to monitor only those spaces that have been identified as requiring video surveillance;

(c) The ability of authorized personnel to adjust cameras shall be restricted so that authorized personnel cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program;

(d) Equipment shall never monitor an area~~s~~ where ~~the~~ individuals have a higher expectation of privacy (e.g. change rooms and washrooms);

(e) Where possible, video surveillance should be restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance;

(f) Reception/recording equipment must be located in a strictly controlled access area. Only authorized personnel shall have access to the controlled area and the reception/recording equipment; and

(g) Every reasonable attempt should be made by authorized personnel to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

2. Notice of Use of Video Systems

In order to provide notice to individuals that video surveillance is in use:

(a) The Library shall display signs, visible to members of the public, at all entrances to a premise where video surveillance is being utilized and/or on the perimeter of the area under video surveillance;

(b) The notification requirements of this sign must inform individuals of:

(i) the legal authority for the collection of personal information;

(ii) the principal purpose(s) for which the personal information is intended to be used; and

(iii) the title, business address, and telephone number of someone who can answer questions about the collection.

3. Personnel Authorized to Operate Video Equipment

DRAFT

Only authorized staff shall be permitted to operate video surveillance systems.

B. Video Equipment/Records

1. Types of Recording Device

The Library may use either recording mechanisms that record information directly on a hard-drive ~~Digital Video Recorders (DVR)~~ or recording mechanisms using a removable/portable storage device ~~time lapse Video Cassette Recorders (VCR)~~ in its video systems. Facilities using video recorders will retain these records in accordance with the specified retention periods.

2. Record Identification

All records (storage devices) shall be clearly identified (labeled) as to the date and location of origin including being labeled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a hard-drive, 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 authorized personnel shall affix a label to each storage device identifying this information.

3. ~~Logbook~~ Record Keeping

~~Each location shall maintain a logbook to record all activities related to video devices and records. Activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material, including the name of the person accessing the system. All logbook entries will detail staff name, date, time and activity. This logbook must remain in a safe and secure location with the video recording equipment. Only authorized personnel or a manager may remove this logbook from the secure location~~ Policy, Planning and Performance Management (PPPM) is the office of record for disclosure requests that are received either electronically or in paper format. Requests are to be scanned,

DRAFT

or photographed and e-mailed to disclosure@torontopubliclibrary.ca. A hard copy is to be delivered to the Data Governance and Privacy Risk Advisor via inter-office mail. Staff are not to retain copies of images on their personal devices. Once an image of a form is sent via e-mail, any existing electronic copies of the image must be destroyed from personal devices.

C. Access to Video Records

1. Access

Access to the video surveillance records~~, e.g. logbook entries, CD, video tapes, etc.~~ shall be restricted to authorized personnel, and only in order to comply with their roles and responsibilities as outlined in the Security Video Surveillance Policy.

2. 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.

3. Formal Access Requests Process

With the exception of requests by law enforcement agencies, all formal requests for video records should be directed to ~~the City Librarian's Office~~ PPPM. Requests are subject to the requirements of MFIPPA and the Library's Access to Information and Protection of Privacy Policy.

4. Access: Law Enforcement

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Law Enforcement Officer must complete the Disclosure of Personal Information Form and forward it to the authorized staff member. The authorized staff member will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to MFIPPA exemptions.

DRAFT

It is important to complete the Disclosure of Personal Information Form when requesting video surveillance footage. The Disclosure of Personal Information Form serves as the record for the request and is maintained and stored by PPPM.

Authorized Library staff are to provide law enforcement with a secure means of accessing video footage, as directed by PPPM in the circumstances.

~~The City Librarian, 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 authorized personnel 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) Whether the record will be returned or destroyed after use by the Law Enforcement Agency.~~

5. Viewing Images

When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be undertaken by an authorized personnel, in a private, controlled area that is not accessible to other staff and/or visitors.

6. Custody, Control, Retention and Disposal of Video Records/Recordings

The Library 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 MFIPPA, which include but are not limited to the prohibition of all Library employees from access or use of information from the video surveillance system, its components, files, or database for personal reasons.

~~With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, the Library must not maintain a copy~~

DRAFT

~~of recordings for longer than the recording systems' 30-day recording cycle.~~

The Library 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.

Records and information collected from the video recording system are subject to the following retention periods under the Library's record retention schedules:

(i) Information will be retained for a maximum of thirty (30) days from the date of the original collection by the video surveillance system, except as described in (ii); and

(ii) Information collected from the video recording system used by the Library or a law enforcement agency as part of a criminal, safety, or security investigation or for evidentiary purposes will be retained for a minimum of one (1) year from the conclusion of the matter for which it has been used.

7. Unauthorized Access and/or Disclosure (Privacy Breach)

Any Library employee who suspects a privacy breach should refer to the Privacy Breach Protocol available on ShareTPL:

Any Library employee who becomes aware of any unauthorized disclosure of a video record in contravention of this Policy, and/or a potential privacy breach has a responsibility to ensure that ~~the City Librarian is immediately informed of the breach~~ PPPM is immediately informed of the breach.

~~The following actions will be taken immediately in accordance with TPL's procedures for managing a privacy breach:~~

DRAFT

- ~~Upon confirmation of the existence of a privacy breach, the City Librarian or designate will notify the Information and Privacy Commission of Ontario (IPC);~~

- ~~TPL staff shall 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 City Librarian or designate in consultation with the Director of the division in which the breach of Policy occurred, shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences;~~

- ~~The divisional Director shall inform the City Librarian, or designate of events that have led up to the privacy breach;~~

- ~~The staff member shall work with the divisional Director and the City Librarian, or designate to take all reasonable actions to recover the record and limit the record's disclosure;~~

- ~~The City Librarian, where required, shall notify affected parties whose personal information was inappropriately disclosed.~~

~~A breach of this Policy may result in disciplinary action up to and including dismissal. A breach of this Policy by service providers (contractors) to the Library, may result in termination of their contract.~~

8. Inquiries 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 PPPM ~~the City Librarian's Office.~~

Accountability

1. The Directors Committee is responsible for:

(a) Approval of the installation of video surveillance cameras

DRAFT

~~2. The City Librarian is responsible for:~~

~~(a) Documenting, implementing, enforcing, monitoring and updating the Library's privacy and access compliance;~~

~~(b) Will report to the Board when video surveillance is being proposed for all locations;~~

~~(c) Preparing annual reports to the Board on all security video surveillance systems installed.~~

2. Directors with responsibilities for facilities management, including the Director for Transformational Projects and the Director for Branch Operations and Customer Experience are responsible for:

   (a) Assessing proposed installations of video surveillance equipment after a Security ~~Threat~~ Video Surveillance Needs Assessment has been completed ~~Recommending to the City Librarian any proposed installation in their department which should be considered as high-profile, and therefore reported to the Board.~~

   (b) ~~Either the Director for Transitional Projects or the Director for Branch Operations and Customer Experience are responsible for Approving proposed installations of video surveillance systems.~~

3. The Director, PPPM ~~Corporate and Service Planning, Policy, and City-Wide Services~~ is responsible for:

   (a) Documenting, implementing, and enforcing the Library's privacy and access compliance policies;

   (b) Responding to formal requests to access records, including law enforcement inquiries;

   (c) Providing advice, training and recommendations to staff to assist in compliance with MFIPPA;

   (d) Undertaking periodic evaluation of TPL's video surveillance systems to ensure compliance with this Policy;

   (e) Reviewing this Policy on a regular basis, and recommending updates as appropriate to the City Librarian;

   (f) Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers; and

DRAFT

(g) Investigating privacy complaints related to video surveillance records, and security/privacy breaches.

~~Providing advice, training and recommendations to staff to assist in compliance with MFIPPA;~~

~~(a) Undertaking yearly evaluation of TPL's video surveillance systems to ensure compliance with this Policy;~~

~~(b) Reviewing this Policy every two years, and recommending updates as appropriate to the City Librarian;~~

~~(c) Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers;~~

~~And, in consultation with the City Librarian, for:~~

~~(d) Responding to formal requests to access records, including law enforcement inquiries;~~

~~(e) Investigating privacy complaints related to video surveillance records, and security/privacy breaches.~~

4. The Director of Transformational Projects, and the Director of Branch Operations and Customer Experience each have the authority to: ~~Information Technology and Facilities is responsible for:~~

   (a) Conducting ~~Security~~ security ~~Threat V~~ video ~~S~~surveillance ~~N~~needs ~~A~~assessments to determine requirement for a video surveillance system;
   (b) Advise ~~ing~~ on installations and operation of video surveillance systems;
   (c) Recommend ~~Assessing~~ proposed installations in accordance with this Policy, and in consultation with the appropriate ~~director~~ Director(s). (see approval at Director's Committee);
   (d) Conduct~~ing~~ periodic internal audits to ensure compliance with this Policy;
   (e) ~~Delegating~~ Delegate the day-to-day operations of video surveillance systems to managers, ~~and~~ ensuring system-wide compliance with this Policy and TPL procedures; and
   (f) ~~Ensuring~~ Ensure that appropriate Facilities and Branch staff are familiar with this Policy, and that training is provided by PPPM to all authorized personnel.

5. ~~Library Service Managers, and Facilities' Managers at Toronto Reference Library, are responsible for~~ Authorized staff are responsible for:

DRAFT

(a) Complying with and adhering to all aspects of this Policy;
(b) Overseeing the day-to-day operation of video surveillance cameras, providing supervision to approved authorized personnel, and ensuring their compliance with all aspects of this Policy;
(c) Ensuring all aspects of the video recording system are functioning properly;
(d) Ensuring that training is provided to ~~the authorized personnel and the authorized staff they supervise~~ their staff via PPPM;
(e) Ensuring that all the staff they supervise are familiar with this Policy;
(f) Ensuring monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location;
~~(g) Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorized personnel;~~
(g) Forwarding all external requests for access to video records to the appropriate authorized staff member;
(h) 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;
(i) Ensuring that access to video surveillance occurs within the rules established by the Security Video Surveillance Procedures;
(j) Ensuring that no video surveillance imagery/records are disclosed without the approval of authorized management/in-charge staff;
(k) Ensuring that no copies of data/images in any format (hard copy, electronic, etc.) are taken from the video recording system without approval from authorized management/in-charge staff ;
(l) Informing appropriate shared facilities' personnel of this Policy's requirements;
(m) Immediately reporting breaches of security/privacy to the City Librarian or designate; and
(n) Forwarding all inquiries from the public about the use of video surveillance or about the Library's Security Video Surveillance Policy to PPPM ~~the City Librarian's Office~~

DRAFT

Appendices

Appendix 1: References
Appendix 2: Definitions
Appendix 3: Contacts

DRAFT

Appendix 1

References

Guidelines for Using Video Surveillance ~~Cameras in Public Places.~~ Information and Privacy Commissioner of Ontario. 2015 ~~2007~~.

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1990, c. M. 56 (MFIPPA).

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1991, Regulation 372/91 as Amended.

Occupational Health and Safety Act, R.S.O. 1990, c.O.1.

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report – Privacy Investigation Report MC07-68, Information and Privacy Commissioner/Ontario, 2008.

Toronto Public Library Access to Information and Protection of Privacy Policy.

Toronto Transit Commission Video Recording Policy for Security Purposes. 2018.

DRAFT

Appendix 2

Definitions

Authorized staff: Employees of Toronto Public Library or of a Toronto Public Library contractor who are specifically authorized by the Library to operate the video surveillance system for a particular facility and to perform the duty, responsibility or action described in the Policy and in the Security Video Surveillance Procedures.

Video surveillance operation: Operation of the video surveillance system may include:

a. Requesting access to video surveillance records
b. Accessing/viewing/retrieving video surveillance records
c. Disposing of video surveillance records
d. Installing/maintaining video surveillance systems and infrastructure

DRAFT

Appendix 3

Contacts

Vickery Bowles, City Librarian, City Librarian's Office
Tel: 416-393-7032
~~: Public inquiries, formal requests for access to records, privacy breaches, complaints~~

Elizabeth Glass, Director, Policy, Planning and Performance Management
Tel: 416-395-5602
~~**Planning, Policy, and E-Service Delivery:** Compliance with MFIPPA;. Fax: 416-393-7083~~

Paul Trumphour, Director, Transformational Projects
Tel: 416-395-5541

Moe Hosseini-Ara, Director, Branch Operations and Customer Experience
Tel: 416-397-5944

~~Director, Information Technology and Facilities: Installation, management and operation of security video surveillance systems.Tel: 416-393-7104~~
~~Fax: 416-393-7083~~

DRAFT

SECURITY VIDEO SURVEILLANCE GENERAL PROCEDURES

The Security Video Surveillance Procedures have been developed to assist Library staff ~~contractors,~~ and service providers to fulfill their roles and responsibilities in accordance with the Security Video Surveillance Policy. Please ensure that you review and follow these procedures carefully along with the Security Video Surveillance Policy before taking any action with respect to the Library's video surveillance equipment.

Video surveillance imagery will only be accessed for the following reasons:

a) Providing video surveillance images to law enforcement agencies for law enforcement proceedings;
b) Investigating health & safety, security, or other incidents not requiring the involvement of law enforcement agencies, in consultation with management staff; and
c) Providing technical troubleshooting support.

Security video surveillance imagery may also be accessed for formal Freedom of Information requests under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Authorized Library Staff

As outlined in the Security Video Surveillance Policy, only authorized Library staff~~, contractors,~~ and service providers may operate security video surveillance systems for a particular facility and perform the duty, responsibility or action described. This includes:

- Operating security video surveillance cameras;
- Reviewing security video surveillance images/recordings;
- Providing security video surveillance images/recordings to law enforcement agencies; and
- Maintaining security video surveillance ~~log books, etc~~ records.

Authorized Library staff are those individuals who have been designated by a Director or the City Librarian to carry out any of tasks a, b, or c listed above. A Director is to confirm such designation in writing.

Library staff authorized for the operation of the security video surveillance system are as follows:

1. Staff authorized to request the extraction of video surveillance images/recordings for reasons a) and/or b), described above include:
    a. City Librarian
    b. All Directors
    ~~c. City Librarian~~

~~d. Director, Branch LibrariesOperations and Customer Engagement~~
~~e. Director, Research & Reference~~
~~f. Director, Information Technology & FacilitiesDigital Services and Emerging Technologies~~
~~g. Director, Collections and Collections Management & City-Wide ServicesMembership Services~~
~~h. Director, Human Resources~~
~~i. Director, Service Development and Innovation~~
~~j. Director, Policy, Planning, and Performance Management~~
~~k. Director, Transitional Projects~~
~~l. Director, Finance and Treasurer~~
~~m. Director, Communication, Programming and Customer Engagement~~
~~n. Senior Manager, Facilities~~
~~o. Senior Manager, Information Technology~~
c. Area Managers
d. Library Service Managers
e. Other staff as authorized by the City Librarian or a Director

~~f. Research & Reference Managers~~
~~g. Manager, Mobile Library Services~~
~~h. Senior Human Resources Consultant~~
~~i. Branch Heads/Senior Department Heads and designated in-charge staff, in consultation with a manager, where available~~

2. Staff authorized to request video surveillance images/recordings for reason c) including: ~~technical support/troubleshooting purposes~~
    a. City Librarian
    b. Director, Digital Services and Emerging Technologies
    ~~c. Director, Information Technology & Facilities~~
    c. Other staff as authorized by the City Librarian or Director, Digital Services and Emerging Technologies
    ~~Senior Manager, Facilities~~
    ~~Designated Facilities Managers~~
    ~~Designated Information Technology Managers~~
3. Staff authorized to perform extraction of video surveillance images/recordings from the security video surveillance system include:
    a. Director, Digital Services and Emerging Technologies ~~Director, Information Technology & Facilities~~
    b. Director, Transformational Projects ~~Senior Manager, FacilitiesDesignated Facilities~~
    c. Manager, Distribution Services
    d. ~~Managers~~ Other staff as authorized by any Director.
    e. Toronto Reference Library Security Site Supervisor (contracted service)
    ~~f.~~

4. ~~North York Central Library Administrative Support Assistant~~Staff authorized to access and view security video surveillance images/recordings for official purposes as described at the beginning of these procedures:
    a. City Librarian
    b. All Directors
    ~~c. Director, Branches~~
    ~~d. Director, Research & Reference~~
    ~~e. Director, Information Technology & Facilities~~
    ~~f. Director, Collections Management & City-Wide Services~~
    ~~g. Senior Manager, Facilities~~
    ~~h. Senior Manager, Information Technology~~
    ~~i. Area Managers~~
    ~~j. Library Service Managers~~
    ~~k. Research & Reference Managers~~
    ~~l. Manager, Mobile Library Services~~
    ~~m. Manager, Distribution Services~~
    ~~n. Facility Operations Managers~~
    ~~o. Branch Heads/Senior Branch Heads/Senior Department Heads~~
    ~~p. Designated in-charge staff~~
    ~~q. Security guards (contracted service)~~
    c. Other Library staff as required and specifically authorized by a member of this list, for individual instances of accessing video surveillance images/recordings as stated in reason b).

Note that video surveillance cannot be accessed for any purpose without the express authorization of an appropriate staff member, as described in lists 1 and 2.

~~When security video images are reviewed, authorized Library staff will record in the log book the reason for reviewing security video images along with other information regarding the date, time, name of authorized Library staff, etc. See log book procedures and log book form for a detailed list of information to be captured.~~ Accessing video surveillance recordings for law enforcement proceedings or internal investigations (including health & safety, security, or other incidents):

Toronto Public Library will make security video images available to law enforcement agencies upon request. TPL ~~and~~ can access and view video surveillance recordings to investigate health & safety, security, or other incidents as required (i.e. for internal investigation). When recorded images from Library security video surveillance cameras must be viewed for any reason, this must only be undertaken by authorized Library staff, in a controlled area that is not accessible to other staff and/or visitors.

If you are required to view or access video surveillance for law enforcement or internal investigations, you should:

a. For requests from law enforcement agencies, provide the law enforcement agency with a *Disclosure of Personal Information – Security Video Record Form* to fill out. This form is available on ShareTPL in the Forms section. The *Disclosure of Personal Information – Security Video Record Form* captures who the image was provided to, under what authority, when this occurred, and if it will be returned or destroyed after use. Note that this form is not required for internal investigations, however, in the event of such an investigation, all remaining steps must still be followed.
b. Contact the Manager in charge of security Transformational Projects ~~of Distribution Services~~ to coordinate the retrieval and delivery of the recording/images, and to provide a copy of the signed request form (if required). Alternatively, if the imagery is from TRL,~~or NYCL,~~ the onsite Security Site Supervisor (TRL) ~~or Administrative Support Assistant (NYCL)~~ can be contacted to coordinate the retrieval of the recording/images.
c. Once filled out, send the signed *Disclosure of Personal Information – Security Video Record Form* in hard copy to the Data Governance and Privacy Risk Advisor. Send a scanned or photographed image of the form via e-mail to disclosure@torontopubliclibrary.ca for record-keeping purposes. If a personal device is used to take a picture of the form, delete the image from your personal phone immediately after sending. ~~*The Manager of Distribution Services will arrange for transfer of a copy of the recording/images to the Privacy & Records Management Officer.*~~
d. For requests from law enforcement agencies, after the *Disclosure of Personal Information – Security Video Record* form has been completed, signed by the requesting law enforcement agency, and returned to the Library, provide the recording/image to the law enforcement agency.
e. All instances of accessing, viewing, or extracting video surveillance imagery for any reason ~~must be documented in the log book. See the log book procedures for a detailed list of the information to be captured.~~are documented via completion of the applicable disclosure request form and maintained by PPPM.
f. Whenever ~~Any time that~~ video surveillance imagery is accessed for violent incidents that occur on library property or ~~involving~~ involve Library staff, an incident report must be completed.~~and the e~~ The extracted video surveillance imagery forms part of that incident report. Confirm that all relevant information is captured in the incident report form, and in any other forms that may be required for the incident or investigation, such as forms required by the Occupational Health and Safety Act or the Workplace Safety and Insurance Act.~~Provide a copy of the recording/image and a copy of the associated incident report to the Privacy & Records Management Officer. For requests from law enforcement agencies, the signed request form must be included.~~

Installation of Video Surveillance Cameras

Please refer to Section A of the Specific Directives listed in the Security Video Surveillance Policy, "Protocol for implementation of a video surveillance system at a particular site ~~Protocol for~~

~~installation of a video surveillance system at a particular site~~" for information on the justification for installing a video surveillance camera. Please note the following:

1) Installation of video surveillance is the responsibility of the facilities manager(s) as designated by the Director, Transformational Projects or the Director, Branch Operations and Customer Experience.

2) Approval of the installation of a video surveillance camera lies with the Director's Committee.

Custody, Control, Retention and Disposal of Security Video Records/Recordings

1) The Library retains custody and control of all original video records not provided to law enforcement agencies.

2) The Library must not maintain video recordings for longer than the recording system's normal recording cycle, not to exceed 30 days, with the exception of copies of records retained for criminal, safety, or security investigations or evidentiary purposes.

3) All tapes or other storage devices that are not in use must be stored securely in a secured receptacle located in an access-controlled area.

~~4) If a video surveillance tape/storage device requires disposal, Library staff should contact Facilities to dispose of the equipment in accordance with technology asset disposal processes (shredding, burning, or erasing depending on the device) to ensure that personal information is erased prior to disposal, and cannot be retrieved or reconstructed.~~

Removing and/or Relocating Security Video Cameras

1) If a security video camera needs to be removed and/or relocated for any reason, including that it is no longer functioning, Library staff should submit a Facilities work~~d~~ order.

2) Security video surveillance cameras must not be removed and/or relocated without the expressed written permission of the Director, ~~IT & Facilities,~~ Transformational Projects or designate.

Labelling Security Video Records

1) All security video records (storage devices) shall be clearly identified (labelled) with the date and location, including a unique sequential number or other verifiable symbol.

2) In locations with a VCR or other recording mechanism using a removable/portable storage device, the authorized personnel shall affix a label to each tape/storage device.

3) In locations with a DVR that stores information directly on a hard-drive, the computer time and date stamp shall be understood to be the label.

Unauthorized Access and/or Disclosure (Privacy Breach)

1) If you become aware of any unauthorized disclosure of a video record and/or a potential privacy breach, your responsibility is to ensure that steps are taken in accordance with the Toronto Public Library Privacy Breach Protocol, available on ShareTPL.
2) Co-ordinate with ~~the City Librarian's Office~~ Policy, Planning and Performance Management in accordance with the Privacy Breach Protocol. ~~is immediately informed of the breach/potential breach.~~

Enquiries

1) Questions regarding installation, management and operation of security video surveillance systems should be directed to the Director, ~~Information Technology and Facilities~~ Transformational Projects.

2) All other questions should be directed to~~the Privacy & Records Management Officer~~ Policy, Planning and Performance Management.

SECURITY VIDEO SURVEILLANCE LOG BOOK PROCEDURES

1) A log book is provided at each location where security video equipment is stored. Additional log book forms can be accessed from the *Forms* section of the ShareTPL.

2) Log books will be kept in a safe and secure location with the video recording equipment.

3) Each location shall maintain a log book to record all activities related to video devices and records. Activities include:
    - All information regarding the use, maintenance, and storage of records
    - All instances of access to and use of recorded material, including the name of the person accessing the system.

4) Only Authorized Library staff will record the activities related to security video surveillance systems in the log book.

5) Information to be captured in the log book includes:
    - The date and time of the original, recorded incident including the designated location name and number (if available) of the applicable camera and VCR/DVR.
    - The name of the authorized staff who requested access to the video surveillance imagery.
    - The time and date the copy of the original record was extracted.
    - The time and date the extracted record was provided to law enforcement agencies.
    - Whether the record will be returned or destroyed after use by law enforcement agencies.

6) A single entry in the log book may have multiple actions taken, e.g., if for a particular incident, law enforcement agencies require video surveillance images for an investigation, the following actions would be recorded in the log book:
    - *Reviewed Security Video Record* - Library staff reviewed the video surveillance record to determine that requested footage is available and on which portion of the tape/recording device.
    - *Extracted Security Video Record*- Library staff copied the portion of the security video record required by law enforcement agencies for investigative or evidentiary purposes onto another tape/storage device.
    - *Removed tape/storage device* – Library staff removed the original tape/storage device and stored it in a secure location until it is no longer required for investigative or evidentiary purposes.
    - *Replaced tape/storage device with a new tape/storage device* – Indicates that Library staff put a new tape/storage device in the recording device

7) The log book is not to be removed from the site unless authorized by the City Librarian's Office.

Process for Acquiring Security Camera Equipment

1. Branch Head/Manager identifies need for new or replacement security camera(s)

2. Emails appropriate Facilities Operations Manager to request a security audit

3. Facilities Operations Manager will conduct the audit along with the appropriate manager:
    a. The Facilities Operations Manager and the Library Service Manager are responsible for completing the assessment forms as follows:
        i. Branch staff/manager complete the *TPL Security Video Surveillance Needs Assessment* form
        ii. Facilities Manager completes *TPL Security Video Surveillance Needs Assessment Results* report and gets a quote from DBS Security Solutions
        iii. Completes an unsigned Purchase Requisition
        iv. Both reports, quote and requisition are sent to Director, Branch Operations & Customer Experience

4. Director, Branch Operations & Customer Experience
    a. Reviews, modifies if required, and approves the request, and forwards the reports to the Director, Transformational Projects

5. Director, Transformation Projects
    a. Reviews the package to ensure the assessment meets policy requirements
    b. Completes a Directors' Committee report seeking authorization for the installation
    c. Following approval signs the Purchase Requisition
    d. Forwards Purchase Requisition to Finance

6. Finance
    a. Issues Purchase Order

7. Facilities Operations Manager
    a. Makes arrangements with vendor for installation
    b. Confirms that work has been completed satisfactorily
    c. Receives invoice
    d. Signs invoice to recommend payment (budget code on invoice from PO)
    e. Forwards invoice to Finance for payment

TPL SECURITY VIDEO SURVEILLANCE SYSTEM
NEEDS ASSESSMENT FORM

Date of Assessment:

Site Information

Library Branch/Department:

Facility type: Stand alone: ☐ Joint facility: ☐

Is the library located in a priority neighbourhood? ☐

Assessment Team

***Interviewee:** **Phone:**
Position:

Department/Branch Head: **Phone:**

Department/Branch Manager: **Phone:**

Needs assessment conducted by: **Phone:**
(Facilities staff)

***The interviewee for the Needs Assessment should be a supervisor or manager who is regularly at the location.**

Background

In the daily operation of its premises, Toronto Public Library is diligent in protecting and maintaining the safety of property, visitors, and employees in various ways such as:

- alert observation by staff,
- foot patrols by security personnel,
- security-conscious design of Library locations,
- safe behaviour training, and
- the consistent application of the Library's Rules of Conduct.

However, in some circumstances, it is determined that the additional protection provided by surveillance cameras is essential in maintaining the lawful and safe use of Library premises.

Under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) any recorded data of an identifiable individual qualifies as "personal information". Visual, audio or other images collected by security video surveillance systems are therefore subject to the Act.

Because video surveillance collects significant personal information about many individuals, the Library has to balance the security benefits of video surveillance with the rights of individuals under the Act to be free from unwarranted collection, access or disclosure of personal data.

Therefore, in any situation where TPL is considering installing a video system to enhance security and/or safety, a needs assessment must be carried out according to the Specific Directives of the TPL Policy Security Video Surveillance Policy. On completion of this form, the Library will determine whether or not a camera can be installed. The criteria for assessment are:

i) the benefits of surveillance substantially should outweigh the reduction of privacy implied by the installation of a video surveillance system
ii) the use of each camera is justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns; and
iii) other means, such as foot patrols, are not feasible or are substantially less effective.

Assessment

1. Is there already a video surveillance system on the site?

YES ☐ **NO** ☐

If yes,

i) Where are cameras located?

ii) Have they been assessed according to the TPL Security Video Surveillance Policy requirements?

YES ☐ **NO** ☐

If no,

iii) Include in assessments and mark as existing.

2. Proposed location of video surveillance.

Q2.	Location(s) under consideration	Reason for concern If more than one desk/area in the specific location is under consideration, give reason for each location.
(a)	Parking lot/garage	
(b)	External approach to library (e.g. pathways)	
(c)	External entrance to library – Staff:	
(d)	External entrance to library – Public	
(e)	External shipping access	
(f)	Internal staff area (e.g. shipping area)	
(g)	Public lobby	
(h)	Circulation Desk(s)	
(i)	Information Desk(s)	
(j)	Stacks/lounge/study area/Le@rning Centre etc. in library	
(k)	Meeting room	
(l)	Corridor/hallway/stairs/ approach to washroom	
(m)	Other	

3. For each camera, please attach a diagram and marked site plan (where available) showing the proposed location and viewing angle of the camera.

4. 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?

Q.	Security Counter-Measure	Yes	No	Comments
(a)	Security Procedures			
(b)	Duress Buttons			
(c)	Door Locking Hardware (e.g. keys)			
(d)	Alarm System			
(e)	Access Control System (e.g. swipe cards, coded access)			
(f)	Signage			
(g)	Security Guard/Officer Patrols			
(h)	Lighting			
(i)	Other:			

5. 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 incident reports available documenting crime or safety concerns?

YES ☐ NO ☐

IF YES, please describe the kinds of incidents, and their frequency e.g. *"five bicycle thefts between January 30th and April 5th"*

IF NO, what safety concerns/property protection have prompted the request for video surveillance, and what record do you have of them?

6. 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. Have any of the following effects and mitigation strategies been considered?

Q4	Effects & Mitigation Strategies	Yes	No	Comments
(a)	Is the location of the proposed camera situated in an area that will minimize privacy intrusion?			
(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)	Other:			

7. 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?

Q5	Measures to Mitigate Effects	Yes	No	Comments
(a)	Will the proposed camera be restricted through hardware or software to ensure that it cannot be used to view areas that have not been assessed?			
(b)	Is the reception/recording 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:			

Any additional comments:

On completion of the assessment:

Facilities:

- Attach a copy of the Security Video Needs Assessment Results Form to the front of this document
- Complete Parts 1 & 2 of the Results Form
- Copy for branch/location
- Forward original to Director responsible for Facilities with a completed costing estimate

POLICY: **SECURITY VIDEO SURVEILLANCE**

SECTION: **Section V – Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56**

MOTION#/DATE: **07 - 057 – March 26, 2007**
18 - xxx – September 24, 2018

Effective Date: September 24, 2018

Table of Contents

DRAFT

DRAFT

Policy Objective

The purpose of the Video Surveillance Policy is to describe Toronto Public Library's installation and use of video surveillance equipment in the interests of privacy, public safety, protection of property, and to maintain a safe and welcoming environment for library customers, staff, and service providers.

Underlying Principles

Underlying the Policy Objective is Toronto Public Library's commitment to maintaining a safe and welcoming environment for staff and members of the public. Toronto Public Library will achieve this through a modern, cohesive security system that strives to minimize intrusions upon the personal privacy of customers, staff, and service providers. Video surveillance is to be deployed on the basis of a formal needs-assessment carried out by designated Toronto Public Library staff. Through the use of a prescribed protocol, designated staff will be empowered to determine how video surveillance equipment will be deployed based on Toronto Public Library's security needs. Video surveillance will only be deployed for identifiable purposes that are consistent with this Policy.

The Security Video Surveillance Policy provides detailed direction concerning the context, procedures, and protocols within which the Library installs and operates surveillance cameras. The Policy ensures that the Library follows the guidelines set out by the Information and Privacy Commissioner of Ontario, and the privacy requirements of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), without compromising the safety and security of Library visitors, staff, and premises.

Policy Statement

This Policy is in place to maintain public safety and security of property through adequate monitoring of library facilities. The deployment of surveillance cameras and monitoring systems is achieved through the consistent use of an evidence based approach to camera deployment. This protocol is detailed under the "Specific Directives" section of this Policy. Video surveillance deployment is guided by the principle of minimal intrusion by video surveillance systems into the daily operation of library facilities. Video surveillance systems are deployed only when needed based on criteria established within the Specific Directives. Library premises are monitored in the

DRAFT

interest of asset protection, and to maintain safe library premises that are welcoming to library staff and visitors.

Scope

This Policy applies to all surveillance camera systems, deployed across all Library-owned and/or leased properties. This Policy does not apply to video surveillance used for employment-related or labour-related information.

Application

This Policy applies to all Toronto Public Library staff and contracted workers. All parties will be made aware of this Policy, their obligation to comply with it, and given instructions in meeting the Policy's requirements.

Specific Directives

A. Protocol for Implementation of a Video Surveillance System at a particular site:

The Toronto Public Library has developed a needs based assessment process for acquisition and installation of a surveillance camera. The documents developed in relation to this are:

A. TPL Security Video Surveillance System Needs Assessment Form;
B. Process for Acquiring Security Camera Equipment

1. Factors to Consider Prior to Using Video

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

(a) The number of verifiable incidents of crime or significant safety concern;
(b) The level of risk to the safety of staff and customers posed by such incidents;
(c) the potential for violation of the Library's Rules of Conduct;
(d) A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable;

DRAFT

(e) On a system-wide basis, a Privacy Impact Assessment (PIA) must be conducted on the effects that the proposed video surveillance may have on personal privacy. The PIA should indicate mitigation strategies to limit adverse effects relating to privacy; and
(f) The proposed design and operation of the video surveillance systems should minimize privacy intrusion.

1. Designing and Installing Video Surveillance Equipment

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

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

2. Notice of Use of Video Systems

In order to provide notice to individuals that video surveillance is in use:

DRAFT

(a) The Library shall display signs, visible to members of the public, at all entrances to a premise where video surveillance is being utilized and/or on the perimeter of the area under video surveillance;
(b) The notification requirements of this sign must inform individuals of:
  (i) the legal authority for the collection of personal information;
  (ii) the principal purpose(s) for which the personal information is intended to be used; and
  (iii) the title, business address, and telephone number of someone who can answer questions about the collection.

3. Personnel Authorized to Operate Video Equipment

Only authorized staff shall be permitted to operate video surveillance systems.

B. Video Equipment/Records

1. Types of Recording Device

The Library may use either recording mechanisms that record information directly on a hard-drive or recording mechanisms using a removable/portable storage device in its video systems. Facilities using video recorders will retain these records in accordance with the specified retention periods.

2. Record Identification

All records (storage devices) shall be clearly identified (labeled) as to the date and location of origin including being labeled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a hard-drive, 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 authorized personnel shall affix a label to each storage device identifying this information.

DRAFT

3. Record Keeping

Policy, Planning and Performance Management (PPPM) is the office of record for disclosure requests that are received either electronically or in paper format. Requests are to be scanned, or photographed and e-mailed to disclosure@torontopubliclibrary.ca. A hard copy is to be delivered to the Data Governance and Privacy Risk Advisor via inter-office mail. Staff are not to retain copies of images on their personal devices. Once an image of a form is sent via e-mail, any existing electronic copies of the image must be destroyed from personal devices.

C. Access to Video Records

1. Access

Access to the video surveillance records shall be restricted to authorized personnel, and only in order to comply with their roles and responsibilities as outlined in the Security Video Surveillance Policy.

2. Storage

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

3. Formal Access Requests Process

With the exception of requests by law enforcement agencies, all formal requests for video records should be directed to PPPM. Requests are subject to the requirements of MFIPPA and the Library's Access to Information and Protection of Privacy Policy.

4. Access: Law Enforcement

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Law Enforcement Officer must complete the Disclosure of Personal Information Form and forward it to the

DRAFT

authorized staff member. The authorized staff member will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to MFIPPA exemptions.

It is important to complete the Disclosure of Personal Information Form when requesting video surveillance footage. The Disclosure of Personal Information Form serves as the record for the request and is maintained and stored by PPPM.

Authorized Library staff are to provide law enforcement with a secure means of accessing video footage, as directed by PPPM in the circumstances.

5. Viewing Images

When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be undertaken by an authorized personnel, in a private, controlled area that is not accessible to other staff and/or visitors.

6. Custody, Control, Retention and Disposal of Video Records/Recordings

The Library 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 MFIPPA, which include but are not limited to the prohibition of all Library employees from access or use of information from the video surveillance system, its components, files, or database for personal reasons.

The Library 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.

DRAFT

Records and information collected from the video recording system are subject to the following retention periods under the Library's record retention schedules:

(i) Information will be retained for a maximum of thirty (30) days from the date of the original collection by the video surveillance system, except as described in (ii); and

(ii) Information collected from the video recording system used by the Library or a law enforcement agency as part of a criminal, safety, or security investigation or for evidentiary purposes will be retained for a minimum of one (1) year from the conclusion of the matter for which it has been used.

7. Unauthorized Access and/or Disclosure (Privacy Breach)

Any Library employee who suspects a privacy breach should refer to the Privacy Breach Protocol available on ShareTPL:

Any Library employee who becomes aware of any unauthorized disclosure of a video record in contravention of this Policy, and/or a potential privacy breach has a responsibility to ensure that PPPM is immediately informed of the breach.

8. Inquiries 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 PPPM.

DRAFT

Accountability

1. The Directors Committee is responsible for:

    (a) Approval of the installation of video surveillance cameras

2. Directors with responsibilities for facilities management, including the Director for Transformational Projects and the Director for Branch Operations and Customer Experience are responsible for:

    (a) Assessing proposed installations of video surveillance equipment after a Security Video Surveillance Needs Assessment has been completed

3. The Director, PPPM is responsible for:

    (a) Documenting, implementing, and enforcing the Library's privacy and access compliance policies;
    (b) Responding to formal requests to access records, including law enforcement inquiries;
    (c) Providing advice, training and recommendations to staff to assist in compliance with MFIPPA;
    (d) Undertaking periodic evaluation of TPL's video surveillance systems to ensure compliance with this Policy;
    (e) Reviewing this Policy on a regular basis, and recommending updates as appropriate to the City Librarian;
    (f) Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers; and
    (g) Investigating privacy complaints related to video surveillance records, and security/privacy breaches.

4. The Director of Transformational Projects, and the Director of Branch Operations and Customer Experience each have the authority to:

    (a) Conduct Security ~~V~~ideo ~~S~~urveillance ~~N~~eeds ~~A~~ssessments to determine requirement for a video surveillance system;
    (b) Advise on installations and operation of video surveillance systems;

DRAFT

(c) Recommend proposed installations in accordance with this Policy, and in consultation with the appropriate Director(s). (see approval at Director's Committee);
(d) Conduct periodic internal audits to ensure compliance with this Policy;
(e) Delegate the day-to-day operations of video surveillance systems to managers, ensuring system-wide compliance with this Policy and TPL procedures; and
(f) Ensure that appropriate Facilities and Branch staff are familiar with this Policy, and that training is provided by PPPM to all authorized personnel.

5. Authorized staff are responsible for:
   (a) Complying with and adhering to all aspects of this Policy;
   (b) Overseeing the day-to-day operation of video surveillance cameras, providing supervision to approved authorized personnel, and ensuring their compliance with all aspects of this Policy;
   (c) Ensuring all aspects of the video recording system are functioning properly;
   (d) Ensuring that training is provided to their staff via PPPM;
   (e) Ensuring that all the staff they supervise are familiar with this Policy;
   (f) Ensuring monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location;
   (g) Forwarding all external requests for access to video records to the appropriate authorized staff member;
   (h) Documenting all information regarding the use, maintenance, and storage of records; including all instances of access to, and use of, recorded material to enable a proper audit trail;
   (i) Ensuring that access to video surveillance occurs within the rules established by the Security Video Surveillance Procedures;
   (j) Ensuring that no video surveillance imagery/records are disclosed without the approval of authorized management/in-charge staff;
   (k) Ensuring that no copies of data/images in any format (hard copy, electronic, etc.) are taken from the video recording system without approval from authorized management/in-charge staff ;
   (l) Informing appropriate shared facilities' personnel of this Policy's requirements;
   (m) Immediately reporting breaches of security/privacy to the City Librarian or designate; and

DRAFT

(n) Forwarding all inquiries from the public about the use of video surveillance or about the Library's Security Video Surveillance Policy to PPPM.

Appendices
Appendix 1: References
Appendix 2: Definitions
Appendix 3: Contacts

DRAFT

Appendix 1

References

Guidelines for Using Video Surveillance, Information and Privacy Commissioner of Ontario. 2015.

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1990, c. M. 56 (MFIPPA).

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1991, Regulation 372/91 as Amended.

Occupational Health and Safety Act, R.S.O. 1990, c.O.1.

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report – Privacy Investigation Report MC07-68, Information and Privacy Commissioner/Ontario, 2008.

Toronto Public Library Access to Information and Protection of Privacy Policy.

Toronto Transit Commission Video Recording Policy for Security Purposes. 2018.

DRAFT

Appendix 2

Definitions

Authorized staff: Employees of Toronto Public Library or of a Toronto Public Library contractor who are specifically authorized by the Library to operate the video surveillance system for a particular facility and to perform the duty, responsibility or action described in the Policy and in the Security Video Surveillance Procedures.

Video surveillance operation: Operation of the video surveillance system may include:

a. Requesting access to video surveillance records
b. Accessing/viewing/retrieving video surveillance records
c. Disposing of video surveillance records
d. Installing/maintaining video surveillance systems and infrastructure

DRAFT

Appendix 3

Contacts

Vickery Bowles, City Librarian, City Librarian's Office
Tel: 416-393-7092 Fax: 416-393-7083

Elizabeth Glass, Director, Policy, Planning and Performance Management Tel: 416-395-5602

Paul Trumphour, Director, Transformational Projects, Tel: 416-395-5541

Moe Hosseini-Ara, Director, Branch Operations and Customer Experience, Tel: 416-397-5944

DRAFT

SECURITY VIDEO SURVEILLANCE GENERAL PROCEDURES

The Security Video Surveillance Procedures have been developed to assist Library staff and service providers to fulfill their roles and responsibilities in accordance with the Security Video Surveillance Policy. Please ensure that you review and follow these procedures carefully along with the Security Video Surveillance Policy before taking any action with respect to the Library's video surveillance equipment.

Video surveillance imagery will only be accessed for the following reasons:

a) Providing video surveillance images to law enforcement agencies for law enforcement activities;
b) Investigating health & safety, security, or other incidents not requiring the involvement of law enforcement agencies, in consultation with management staff; and
c) Providing technical troubleshooting support.

Security video surveillance imagery may also be accessed for formal Freedom of Information requests under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Authorized Library Staff

As outlined in the Security Video Surveillance Policy, only authorized Library staff, contractors, and service providers may operate security video surveillance systems for a particular facility and perform the duty, responsibility or action described. This includes:

- Operating security video surveillance cameras;
- Reviewing security video surveillance images/recordings;
- Providing security video surveillance images/recordings to law enforcement agencies; and
- Maintaining security video surveillance records.

Authorized Library staff are those individuals who have been designated by a Director or the City Librarian to carry out any of tasks a, b, or c listed above. A Director is to confirm such designation in writing. Library staff authorized for the operation of the security video surveillance system are as follows:

1. Staff authorized to request the extraction of video surveillance images/recordings for reasons a) and/or b), described above include:
    a. City Librarian
    b. All Directors
    c. Area Managers
    d. Library Service Managers
    e. Other staff as authorized by the City Librarian or a Director

2. Staff authorized to request video surveillance images/recordings for reason c) includes:
    a. City Librarian
    b. Director, Digital Services and Emerging Technologies
    c. Other staff as authorized by the City Librarian or Director, Digital Services and Emerging Technologies

3. Staff authorized to perform extraction of video surveillance images/recordings from the security video surveillance system include:
    a. Director, Digital Services and Emerging Technologies
    b. Director, Transformational Projects
    c. Manager, Distribution Services
    d. Other staff as authorized by any Director.
    e. Toronto Reference Library Security Site Supervisor (contracted service)

4. Staff authorized to access and view security video surveillance images/recordings for official purposes as described at the beginning of these procedures:
    a. City Librarian
    b. All Directors
    c. Other Library staff as required and specifically authorized by a member of this list, for individual instances of accessing video surveillance images/recordings as stated in reason b).

Note that video surveillance cannot be accessed for any purpose without the express authorization of an appropriate staff member, as described in lists 1 and 2.

Accessing video surveillance recordings for law enforcement proceedings or internal investigations (including health & safety, security, or other incidents):

Toronto Public Library will make security video images available to law enforcement agencies upon request. TPL can access and view video surveillance recordings to investigate health & safety, security, or other incidents as required (i.e. for internal investigation). When recorded images from Library security video surveillance cameras must be viewed for any reason, this must only be undertaken by authorized Library staff, in a controlled area that is not accessible to other staff and/or visitors.

If you are required to view or access video surveillance for law enforcement or internal investigations, you should:

a. For requests from law enforcement agencies, provide the law enforcement agency with a *Disclosure of Personal Information – Security Video Record Form* to fill out. This form is available on ShareTPL in the Forms section. The *Disclosure of Personal Information – Security Video Record Form* captures who the image was provided to, under what authority, when this occurred, and if it will be returned or destroyed after use. Note that this form is not required for internal investigations,

however, in the event of such an investigation, all remaining steps must still be followed.

b. Contact the Manager in charge of security within Transformational Projects to coordinate the retrieval and delivery of the recording/images, and to provide a copy of the signed request form (if required). Alternatively, if the imagery is from TRL the onsite Security Site Supervisor (TRL) can be contacted to coordinate the retrieval of the recording/images.

c. Once filled out, send the signed *Disclosure of Personal Information – Security Video Record Form* in hard copy to the Data Governance and Privacy Risk Advisor. Send a scanned or photographed image of the form via e-mail to disclosure@torontopubliclibrary.ca for record-keeping purposes. If a personal device is used to take a picture of the form, delete the image from your personal phone immediately after sending.

d. For requests from law enforcement agencies, after the *Disclosure of Personal Information – Security Video Record* form has been completed, signed by the requesting law enforcement agency, and returned to the Library, provide the recording/image to the law enforcement agency.

e. All instances of accessing, viewing, or extracting video surveillance imagery for any reason are documented via completion of the applicable disclosure request form and maintained by PPPM.

f. Whenever video surveillance imagery is accessed for violent incidents that occur on Library property or involve Library staff, an incident report must be completed. The extracted video surveillance imagery forms part of that incident report. Confirm that all relevant information is captured in the incident report form, and in any other forms that may be required for the incident or investigation, such as forms required by the Occupational Health and Safety Act or the Workplace Safety and Insurance Act.

Installation of Video Surveillance Cameras

Please refer to Section A of the Specific Directives listed in the Security Video Surveillance Policy, "Protocol for implementation of a video surveillance system at a particular site for information on the justification for installing a video surveillance camera. Please note the following:

1) Installation of video surveillance is the responsibility of the facilities manager(s) as designated by the Director, Transformational Projects or the Director, Branch Operations and Customer Experience.

2) Approval of the installation of a video surveillance camera lies with the Director's Committee.

Custody, Control, Retention and Disposal of Security Video Records/Recordings

1) The Library retains custody and control of all original video records not provided, in response to a specific legal obligation to produce original records, to law enforcement agencies.

2) The Library must not maintain video recordings for longer than the recording system's normal recording cycle, not to exceed 30 days, with the exception of copies of records retained for criminal, safety, or security investigations or evidentiary purposes.

3) All tapes or other storage devices that are not in use must be stored securely in a secured receptacle located in an access-controlled area.

Removing and/or Relocating Security Video Cameras

1) If a security video camera needs to be removed and/or relocated for any reason, including that it is no longer functioning, Library staff should submit a Facilities work order.

2) Security video surveillance cameras must not be removed and/or relocated without the expressed written permission of the Director, Transformational Projects or designate.

Labelling Security Video Records

1) All security video records (storage devices) shall be clearly identified (labelled) with the date and location, including a unique sequential number or other verifiable symbol.

2) In locations with a recording mechanism using a removable/portable storage device, the authorized personnel shall affix a label to each storage device.

3) In locations with a DVR that stores information directly on a hard-drive, the computer time and date stamp shall be understood to be the label.

Unauthorized Access and/or Disclosure (Privacy Breach)

1) If you become aware of any unauthorized disclosure of a video record and/or a potential privacy breach, your responsibility is to ensure that steps are taken in accordance with the Toronto Public Library Privacy Breach Protocol, available on ShareTPL.

2) Co-ordinate with Policy, Planning and Performance Management in accordance with the Privacy Breach Protocol.

Enquiries

1) Questions regarding installation, management and operation of security video surveillance systems should be directed to the Director, Transformational Projects.

2) All other questions should be directed to Policy, Planning and Performance Management.