Exhibition Place

FORMERLY CALLED:	Security Surveillance Policy V.01

DATE OF ISSUANCE		
March	12	2015

SUPERCEDES POLICY DATED		
July	16	2007

PAGE		
1	of	22

Policy Statement

The Board of Governors of Exhibition Place recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of employees, clients, visitors and property. While video surveillance cameras are installed for safety and security reasons, the Board'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 the Board's facilities and properties operating in a safe, secure, and privacy protective manner.

Policy Description

This policy has been adapted from the City of Toronto's policy and is designed to govern video surveillance at Exhibition Place 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 on the grounds of Exhibition Place installed by Exhibition Place, as well as those proposed to be installed by tenants and event providers and which will survey areas outside of the their exclusive tenanted or licensed areas.

This policy does not apply to cameras used by the Toronto Police Service; or, to video surveillance used for employment related or labour-related information.

Roles and Responsibilities

Responsibilities of Director, Security Services

The Director, Security Services may delegate various responsibilities under this Policy to Division Heads. The key responsibilities of the Director, Security Services include:

- Ensuring Board-wide Policy compliance.
- Undertaking yearly evaluations of video surveillance system installations to ensure compliance with this Policy.
- Reviewing the Policy every two years.
- Approving installation of video cameras at specified locations.
- Receiving status updates from the Manager, Security Services, every six months, regarding staff adherence to the responsibilities within the Policy.
- Reporting to the CEO 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 Services

As designated by the Director, Security Services, the Manager, Security Services, shall:

- Conduct Security Threat Assessments to determine the requirement for a video surveillance system.
- Prepare recommendations for the Director, Security Services for review and installation approval of video surveillance systems.
- Advise the Director, Security Services, on placement of video surveillance monitoring signs.
- Delegate day-to-day operations of video surveillance systems to Security Supervisory staff.
- Conduct periodic internal audits to ensure compliance with Policy.
- Act as contact for all requests by law enforcement agencies for access to video records.
- In consultation with the Manager, Records and Archives / Freedom of Information Coordinator (FIC) and the Director, Security Services develop/update annually privacy training for Board and contract staff who have responsibilities under this Policy.
- In consultation with the Director, Security Services and Manager, Records and Archives / FIC, provide training annually to all Security staff regarding obligations and compliance with MFIPPA and the Policy.
- Immediately report all alleged privacy breaches to the Director, Security Services and the Manager, Records and Archives / FIC for immediate action.
- Consult with the Director, Security Services and forward complaints to the Manager Records and Archives / FIC for appropriate action.

Responsibilities of Supervisor, Security Services

The responsibilities of the Supervisor, Security Services include:

- Overseeing day-to-day operations of video surveillance cameras.
- Ensuring Security Guard's compliance with all aspects of the Policy.
- Ensuring monitoring and recording devices are secured appropriately.
- Recording all activities related to video devices and records, are kept and maintained by operators.
- 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.

Responsibilities of Security Guards

The responsibilities of the Security Guards include:

- Complying and adhering to all aspects of the Policy.
- Monitoring the video surveillance cameras.
- Ensuring all aspects of the video surveillance system are functioning properly.
- Ensuring that no personal information is disclosed without the approval of the Manager, Security Services.
- Ensuring that no copies of data / images in any format (hardcopy, electronic, etc.) are taken from the video surveillance system without approval from the Manager, Security Services.
- Forwarding all requests for access to video records to the Manager, Security Services.

Responsibilities of Manager, Records and Archives/ FIC

The responsibilities of the Manager Records and Archives / FIC in include:

- Providing advice and recommendations to Security Services to assist in compliance with MFIPPA.
- Processing access requests from non-law enforcement agencies for video surveillance records.
- Responding to privacy complaints related to video installations.
- Investigating video surveillance security / privacy breaches.
- In consultation with Manager, Security Services provide training annually to Security Services regarding obligations and compliance with MFIPPA and the Security Video Surveillance Policy (See Appendix #6: Video Surveillance Policy Checklist).

Responsibilities of all Board Staff

All Board staff must adhere to the Policy and must not 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 this 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 cameras, 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 Board's facilities and the need to provide for the safety and security of employees, visitors and clients who may be present at all hours of the day, the Board's video surveillance systems may operate at any time in a 24 hour period.
- The video equipment should be installed to monitor those spaces that have been identified through the Threat Assessment process as outlined in Appendix #5 as requiring video surveillance.
- The ability to adjust cameras should be restricted, if possible, so that the cameras cannot be adjusted or manipulated 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).
- Reception / recording equipment must be located in a strictly controlled access area. Only Security Services staff or those properly authorized in writing by the Director, Security Services shall have access to the controlled area and the reception / recording equipment.

- Every reasonable attempt should be made by system operators to ensure video monitors are not in a position that enables the public and / or unauthorized staff to view the displays.

Notice of Use of Video Systems

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

- The Board shall post visible to members of the public, at all entrances and / or the perimeter of the grounds, signs which prominently indicate that video surveillance is in effect.

- The notification requirements of these signs 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 and contractors designated by the Manager, Security or the Director, Security Services shall be permitted to operate video surveillance systems.

Video Equipment / Records

Types of Recording Devices

Exhibition Place may use either Digital Video Recorders (DVR) or Network Video Recorders (NVR) in its security video surveillance systems. Facilities using video recorders will retain these records for a period of 30 days depending on the recording device and technology. A record of an incident will only be stored longer than the 30 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 (labeled) as to the date and location of origin including being labeled with a unique, sequential number or other verifiable symbol. When using a DVR/NVR that stores information directly on a hard drive, the computer time and date stamp shall be understood to be this identification. When exporting recordings using a removable / portable storage device, the operator shall affix a label to each storage device identifying this information.

Logbook

Every 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 as determined by the Manager, Security Services.

Access to Video Records

Access

Access to the video surveillance records shall be restricted to authorized personnel only in accordance with their responsibilities as outlined in this Policy.

Storage

All video surveillance records 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 Manager, Records and Archives / FIC 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 Manager, Records and Archives / FIC. 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 Exhibition Place, upon a reasonable effort, to identify the record; and,

- At the time of making the request, pay the prescribed fees as provided for under MFIPP.

Access: Law Enforcement

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Law Enforcement Agent must complete the Exhibition Place Law Enforcement Request Form (See Appendix #1) and forward this form to the Manager, Security Services or designate. The Manager, Security Services or designate, will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Agent.

The Manager, Security Services or designate, will record the following information in the facility's logbook:

i) the date and time of the original, recorded incident including the designated name/number of the applicable camera and recording device;
ii) the name of the law enforcement agent making the request;
iii) the time and date the copy of the original record was prepared and sealed;
iv) the time and date the sealed record was provided to the requesting law enforcement agent (chain of custody record)
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 Manager, Security Services in a private, controlled area that is not accessible to other staff and / or visitors.

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

Exhibition Place 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 Board staff 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 Board must not maintain a copy of recordings for longer than the recording systems' 30 day recording cycle.

Exhibition Place 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)

Exhibition Place 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 Services, Director, Security Services and the Manager, Records and Archives / FIC. After this unauthorized disclosure or potential privacy breach is reported:

- Upon confirmation of the existence of a privacy breach, the Manager, Records and Archives / FIC shall notify the Information and Privacy Commissioner 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 Services shall inform the Manager, Records and Archives / FIC 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 Services and Manager, Records and Archives / FIC to take all

reasonable actions to recover the record and limit the record's disclosure.

- When required, the Manager, Records and Archives / FIC, in consultation with the Manager, Security Services will notify affected parties whose personal information was inappropriately disclosed.

- The Manager, Records and Archives / FIC, in consultation with the Manager, Security Services 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 Exhibition Place may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by service providers (contractors) to Exhibition Place, may result in termination of their contract.

Inquiries From the Public Related to the Video Surveillance Policy

A staff member receiving an inquiry from the public regarding the Security Video Surveillance Policy shall direct the inquiry in writing to the Manager, Security Services at ManagerSecurityServices@explace.on.ca.

Review of Video Surveillance Policy

This Policy shall be reviewed every two years by the Director, Security Services.

Approved By:

Date Approved:

Appendix 1 - Law Enforcement Agency Request Form

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

TO: Manager, Security, Exhibition Place.

I, _____, of the _____
Law Enforcement Agent Law Enforcement Agency

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 occur.

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

_____	_____
Manager, Security Services or Designate Releasing Recording	Signature of Manager, Security Services or Designate Releasing Recording

Return all completed ORIGINAL forms to the Manager, Security Services, Exhibition Place, Toronto, Ontario, M6K 3C3. Should you have any questions regarding the use of this form, please call (416) 263-3638.

Exhibition Place

[redacted]

Appendix 2 – Access / Correction Request

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

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 Board of Governors of Exhibition Place. Forward to the Manager Records and Archives / FIC at 100 Princes' Blvd Suite 1, Exhibition Place Toronto, ON M6K 3C3.

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

Request for:

☐ Access to General Records — Identify Dept.: _____

☐ Access to Own Personal Information — Other Institution: _____

☐ Correction of Own Personal Information — (If applicable)

Last Name	First Name	Initial	Daytime Phone No.
			( )

Address	Suite	City/Town	Prov.	Postal Code	Evening Phone 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

Date Request Received

_____	_____	_____
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 Manager Records and Archives / FIC, at (416) 263-3658.

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: records;	$7.50 per ¼ hour required to search and retrieve
Record Preparation (i.e. severing): release;	$7.50 per ¼ hour required to prepare records for
* 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.

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 Exhibition Place are immediately notified of the breach, including your direct supervisor, the Manager, Security Services and the Director, Security Services.

- 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 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 Manager, Security Services and Manager, Records and Archives / FIC, determine whether the privacy breach could allow unauthorized access to any other personal information.

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

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

- Identify those individuals whose privacy was breached.
- 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

- The Manager, Records and Archives / FIC will inform the Information and Privacy Commissioner of Ontario (IPC) Registrar of the privacy breach and advise of immediate containment and notification actions taken by Exhibition Place.

- The Manager Records and Archives / FIC, in consultation with the IPC and department staff will conduct an internal investigation. The objective 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.

- The Manager Records and Archives / FIC 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 Board of Governors of Exhibition Place and are intended to provide basic information on how to proceed in the event of a privacy breach.
For more information about appendix #4, please contact the Manager Records and Archives / FIC at 416 263-3658.

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. Does a video surveillance system and / or camera currently exist on site? If so, please describe and advise if its' set-up adheres to the Board of Governors of Exhibition Place 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 Patrols	☐	☐	
H	Lighting	☐	☐	
I	Other: (Crime Prevention Through Environmental Design, 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	Security Occurrence Reports	☐	☐	
B	Police Reports	☐	☐	
C	H&S Consultants Reports	☐	☐	
D	OH&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?	☐	☐	
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 system 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 a way that it will be hidden from public view?	☐	☐	
D	Other:	☐	☐	

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 Exhibition Place's Security 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 Board of Governors of Exhibition Place intends to meet these obligations through the use of this Training Checklist and formal training completed annually.

1. Policies and Procedures

#	Question	Yes	No	Comments
A	Has received a copy of, read and understood the Security Video Surveillance Policy of Exhibition Place?	☐	☐	
B	Has received a copy of, read and understood the applicable appendices to Exhibition Place'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 Director, Security Services; the Manager, Security Services; the Security Supervisors, the Manager, Records and Archives / FIC;	☐	☐	
B	Understands and will adhere to staff obligations as outlined in the Act	☐	☐	

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 Exhibition Place's Security Video Surveillance Policy?	☐	☐	
B	Is aware that 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 is maintained	☐	☐	
C	Is aware that information regarding the use, maintenance, and storage of records in the logbook, including all instances of access to, and use of recorded material is maintained.	☐	☐	
D	Is aware that deliberately entering false or incomplete information or deleting existing information in any logbook is an unauthorized action that would cause the destruction or alteration of any information contained in any logbook?	☐	☐	
E	Is aware that no changes may be made 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 no copies may be made of data/images in any format (hardcopy, electronic, etc) from the video surveillance system without approval from the Manager, Security Services following the protocols set out in the Video Surveillance policy?	☐	☐	

5. Access to Video Surveillance Records

#	Question	Yes	No	Comments
A	Is aware that access to information is on a need to know basis as determined by the Manager, Security Services or designate for the performance of their duties?	☐	☐	
B	Is aware that access or use information from any component(s) of the Video Surveillance system files or database for personal reasons Is in breach of the Act	☐	☐	
C	Is aware that access to the video surveillance records e.g. logbook entries, CD's, external memory devices, etc. shall be restricted to authorized personnel only?	☐	☐	
D	Is aware that disclosure of personal information should only occur by the Manager, Security Services or designate in consultation, as necessary, with the Manager Records and Archives / FIC 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 Agency 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 unauthorized 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 the disposal , destruction, or erasure of any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy is in contravention of the Act	☐	☐	
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, Exhibition Place 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 day period depending upon the type of technology for non-incident recording.	☐	☐	
D	Understands that all reasonable efforts shall be taken to ensure the security of records in their 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 Exhibition Place staff who become aware of any unauthorized disclosure of a video surveillance record in contravention of the Video Surveillance Policy of Exhibition Place and / or a potential privacy breach are to immediately notify the Manager, Security Services and their direct supervisor.	☐	☐	
B	Understands that intentional wrongful disclosure, or disclosure caused by negligence, by employees Exhibition Place	☐	☐	

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

9. Inquiries from the Public

#	Question	Yes	No	Comments
A	Is aware that any employee receiving an inquiry from the public regarding the Security Video Surveillance Policy shall direct the inquiry to the Manager, Security Services at ManagerSecurityServices@explace.on.ca	☐	☐	

10. Audit

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

_____	_____	_____
Employee / Provider (print)	Signature	Date
_____	_____	_____
Witnessed by (Print)	Signature	Date

Version Number: V.02

Version Date: March 12th, 2015

Created By: Edward Wiersma – Manager, Security Services

Approved By: Francesca Colussi – Director, Parking and Security Services

Procedure Approval:

_____ _____

Edward Wiersma – Manager, Security Services Date:

_____ _____

Francesca Colussi – Director, Parking and Security Services Date: