| | |
|---|---|
| **POLICY TITLE** | CCTV Systems |
| **CATEGORY** | Administrative |
| **POLICY NUMBER** | ADMIN 016 |
| **POLICY OWNER** | City Clerk's Office – Access to Information and Privacy |
| **ACCESS** | Internal only |

## PURPOSE

This policy is intended to ensure that any use by the City of closed-circuit television or other video systems (CCTV systems) appropriately respects privacy, protects personal information captured by the CCTV systems, and complies with the City of Vancouver's Privacy Policy and all applicable laws, such as the Freedom of Information and Protection of Privacy Act (*FIPPA*).

## SCOPE

This policy applies to all CCTV systems owned or operated by the City, or by its related boards and commissions, and all third party systems installed on City premises, with the exception of CCTV systems owned or operated by the
Vancouver Police Department (VPD) and the Vancouver Public Library, (VPL).

## DEFINITIONS

For the purposes of this policy:

**"Applicant"** means the General Manager of the responsible department or his or her delegate.

**"CCTV Application"** means the form that must be completed and approved prior to installing cameras, also known as a CCTV privacy impact assessment, (PIA).

**"CCTV Application Amendment"** means the form that details changes to an approved CCTV Application that must be completed and approved prior to implementation of the changes.

**"CCTV system"** refers to any mechanical, electronic or digital system or device that: (i) enables continuous or periodic CCTV or video recording, observing or monitoring of individuals, assets and/or property; and (ii) is intended to be

mounted or affixed to a structure, fixture or vehicle. For greater certainty, "CCTV system" includes devices such as enterphone systems, handheld license plate recognition systems and drones, but does not include cell phones with video capability, hand-held video recorders or video conferencing systems.

**"FIPPA"** means the *Freedom of Information and Protection of Privacy Act*

**"Head"** means the City Manager, or the Director, Access to Information and Privacy, as designated under the *Freedom of Information and Protection of Privacy By-law* and

Delegation by the Head of the City of Vancouver.

**"Personal information"** means recorded information about an identifiable individual including, but not limited to, information relating to an individual's appearance and activities.

"**Public event**" means a presentation, ceremony, performance, sports meet or similar event at which the individuals voluntarily appear and that is open to the public.

**"Responsible Department"** means the department that is submitting the application for a CCTV system and is using the CCTV system.

## POLICY STATEMENTS

### 1 General Principles

All CCTV systems must be used in accordance with the provisions of *FIPPA*.

A CCTV Application is required for all CCTV systems, whether or not they collect personal information.

CCTV monitoring systems must not be used to monitor staff attendance or performance except as specifically permitted and authorized pursuant to this policy. In the event that this policy is inconsistent with the terms of any collective agreements between the City and its Unions regarding the use of CCTV monitoring, the terms of any collective agreements will take precedence.

The City Manager has been designated as the Head of the City for the purpose of *FIPPA*. The Director, Access to Information & Privacy (ATIP) has been delegated the authority to exercise all powers, duties and functions of the Head in relation to City CCTV systems.

The Director, Access to Information & Privacy, (ATIP) has overall responsibility for all City CCTV systems, but the General Manager of the Responsible Department will be responsible for the operation of each CCTV system used by their department unless otherwise specified in the

CCTV Application or CCTV Amendment Application.

Only authorized employees are permitted to operate or monitor CCTV Systems and/or access CCTV footage. CCTV Applications must provide full and complete detail regarding access authorizations.

The Responsible Department must maintain a log for the operation of their specific CCTV system, showing the dates and times of operation, the location and field of view of the cameras, and the position titles of those that have access to the information.

## 2 Privacy and transparency

The City acknowledges that CCTV systems are privacy intrusive and may only be used when other less intrusive options will not be effective as detailed below. The City will exercise a high degree of care when using CCTV systems to ensure that such systems are authorized and operate in a privacy protective manner.

*FIPPA* requires the City to notify individuals when their personal information may be collected unless a specific exception applies. The method used to give notice will be consistent with the location, use and purpose of the CCTV system.

## 3 Collection of personal information

Personal information must only be collected as permitted under *FIPPA*.

Other than at a public event, a CCTV system that collects or may collect personal information may be used only when it is directly related to and necessary for a City program or activity, such as maintaining the safety or security of individuals, assets or property or to maintain public safety. A CCTV system will only be considered necessary where there is no less intrusive method that can reasonably meet the requirements of the program or activity.

If the original purpose for which a CCTV system was approved is no longer applicable or the system no longer meets the above criteria, the CCTV system must be discontinued. Discontinued systems must be disabled and removed. No non-functioning system should remain to imply security protection.

The CCTV Application or CCTV Application Amendment also serves as a Privacy Impact Assessment for *FIPPA* purposes.

A CCTV Application must be completed and approved before implementing a new CCTV system. A CCTV Application Amendment must be completed and approved before any material change in use or purpose of an existing CCTV system. The CCTV Application or CCTV Application Amendment must identify the City program or activity that requires the system, or the public event at which it will be used, or

certify and demonstrate that the system will not collect personal information under any circumstances.

## 4 Approval

All new CCTV systems, or significant changes or expansions to existing CCTV systems, must be approved in advance by the Head.

To obtain approval, an Applicant must submit a CCTV System Application or a CCTV Application Amendment to the Access to Information and Privacy Division of the City Clerk's Office.

The form and content of the CCTV System Application or CCTV Application Amendment will be set by the Head.

## 5 Documentation

The following information must be maintained by the Access to Information and Privacy Division of the City Clerk's Office:

(a) The original CCTV Application for a new system or expansion of an existing system; and

(b) The CCTV Application Amendment for changes to or expansion of an existing system.

The Responsible Department must maintain the following information:

(a) A copy of the CCTV Application for a new system; and

(b) A copy of the CCTV Application Amendment for changes to or expansion of an existing system;

(c) operating records and logs required by this policy and any applicable procedure under this policy;

(d) a map of camera locations and approximate coverage area(s); and

(e) any other documents or records identified in an applicable procedure under this policy or identified in the system's operating procedures.

Information may be released to the public through the freedom of information process, or as otherwise required by law. Freedom of information requests are the responsibility of the Access to Information and Privacy Division, City Clerk's Office and must be directed there.

## 6 Installation and Placement

Installation and placement of cameras must minimize any potential invasion of privacy. In particular, the following considerations must guide the installation and placement of video monitoring equipment:

a) Cameras must be installed in such a way that they only monitor those areas that have been identified as requiring video monitoring.

b) Adjustment of camera positions and field of view must be restricted, if possible, to ensure only designated areas are being monitored.

c) Video monitoring must be restricted to those time periods when the system is serving its intended purpose, as set out in the CCTV Application, or CCTV Application Amendment.

d) Where operationally feasible, access to areas in which video systems may be monitored must be restricted to authorized employees.

e) CCTV system servers and recordings must be stored in secured locations and be accessible only to authorized employees.

## 7 Use, Access, and Disclosure

Information recorded by a CCTV system may only be used, disclosed, or accessed for the purpose for which it was collected or as otherwise authorized by law.

Only the Head or the position(s) specified in the approved CCTV Application or CCTV Application Amendment may authorize disclosure of information recorded by a CCTV system. In order to enable a proper audit trail, logs must be kept of any such instance of disclosure.

The information recorded by CCTV systems is subject to *FIPPA*. Access requests that are not compliant with *FIPPA* and/or this Policy, must be forwarded to the Access to Information and Privacy Division, City Clerk's Office.

Unauthorized access to, use or disclosure of personal information from a CCTV system is a breach of this policy and the Privacy Policy.

## 8 Logs and audits

For each CCTV system that collects or may collect personal information, the log must also record all viewings of CCTV System recordings, the start and end locations viewed in the recording, the date and time of viewing, and identities of all individuals who have viewed the video.

Audits of systems that collect personal information will be conducted by Internal Audit on a regular basis in order to confirm compliance with

*FIPPA* and adherence to this policy and the associated procedures. Those viewing a CCTV system must be made aware that each system is subject to random auditing and that they may be called upon to justify the method and details of use of the system.

## 9 Service Providers

The General Manager of the Responsible Department, or other position(s) specified in the approved CCTV Application or CCTV Application Amendment, is responsible for ensuring that any service provider responsible for installation or operation of a CCTV system used by their department is made aware of, and complies with, this policy, any applicable procedure, and the statutory obligations of a service provider to a public body under *FIPPA*.

## 10 System Security

The City is responsible for securing all CCTV systems and all personal information they collect, to protect against risks such as unauthorized access, collection, use, disclosure or disposal of any personal information.

## 11 Reporting

The Head will report in writing to Council annually regarding any significant breaches of this policy which could materially impact an individual or the City.

## 12 Data Sharing

The City may enter into agreements to share live feeds of CCTV system video with other governmental agencies, with prior approval of the Head provided that it be a condition of such an agreement that the other governmental agency not be permitted to record the CCTV system video.

## 13 CCTV System Procedures

The Head may make and amend procedures in furtherance of and not inconsistent with this policy.

## 14 Records Management

Records created by CCTV systems are subject to *FIPPA*, the Records Management By- law, the Corporate Records and Information Management Policy and VanRIMS classifications which prescribe retention periods. The General Manager of each Responsible Department with a CCTV system, or the position(s) specified in the approved CCTV Application or CCTV Application Amendment, is responsible for ensuring adherence to the prior noted Records Management Policies and By-laws as well as alignment with Records Management under this policy.

All CCTV recordings must be retained for a period of no longer than 65 days and destroyed at the end of this retention period unless:

a) the recorded information reveals an incident that contains personal information about an individual and the City uses this information to make a decision that directly affects the individual, in which case the CCTV records must be retained for one year after the decision is made in accordance with the *FIPPA*;

b) a request is made by the City's Legal Services Department or Risk Management Department to preserve the recorded information on the basis that the recorded information is relevant to contemplated or current litigation, in which case the CCTV records must be retained until:

    (i) 10 days after the expiry of the applicable limitation period for the commencement of a legal action where a legal action is contemplated but no legal action is commenced;

    (ii) 10 days after the expiry of the applicable appeal period where a legal action has been commenced, the matter has been adjudicated upon by the Court or an administrative tribunal and no appeal has been filed; or

    (iii) 10 days after the settlement or other resolution of the litigation.

c) the Responsible Department requires the CCTV recordings to be preserved for an additional period of time in order to complete the business purpose for which the CCTV recordings were created. In such a case, the Applicant must make a written request to the Director ATIP setting out the basis on which an extension is required. Upon receipt of the request, the Director ATIP may decline or grant the request for an extension to a fixed date.

The Access to Information and Privacy Division, City Clerk's Office is the office of primary responsibility for CCTV privacy impact assessments as contained in CCTV Applications or CCTV Amendment Applications created pursuant to this policy. The Office is also responsible for Freedom of Information requests related to records that the City collects via its CCTV systems.

## 15 Breach of Policy

Complaints about breach of this policy must be made to the Director ATIP who will give notice of the complaint to the General Manager of the Responsible Department. The Director ATIP, or their delegate, may carry out an investigation. Where it is alleged that the breach was by an employee and an investigation is to take place, Human Resources will be notified in advance of the investigation.

After the investigation, the investigator will prepare a written report appropriate to the degree of the alleged breach.

In an appropriate case, the report may contain finding of facts, and recommendations aimed at ensuring that the policy or procedure will be followed in future.

A copy of the report will be provided to the General Manager of the Responsible Department, the Head, the complainant and to the person alleged to have breached the Policy.

Breach of this Policy or of any procedure created pursuant to it by an employee may result in discipline up to and including discharge.

Breach of this Policy or of any procedure created pursuant to it by any person may result in legal proceedings, including criminal prosecution.

The Head is responsible for initiating discipline or legal action for a breach of this policy.

## REFERENCES

Freedom of Information and Protection of Privacy Act
Records Management By-law No. 9067
Freedom of Information and Protection of Privacy By-Law No. 11451

## RELATED POLICIES AND PROCEDURES

| | |
|---|---|
| ADMIN-009 | Corporate Records and Information Management Policy |
| ADMIN-029 | Privacy Policy |
| ADMIN-016P1 | Procedure for Public Realm CCTV Systems |
| ADMIN-016P2 | Procedure for CCTV Monitoring of City Premises |
| ADMIN-016P3 | Procedure for Traffic CCTV Systems |

**APPROVAL HISTORY**

| | | | |
|---|---|---|---|
| **Issued by:** City Manager's Office | **APPROVED BY:** | City Clerk, Head, Freedom of Information and Protection of Privacy | **Date:** **March 26, 2015** |
| | **APPROVED BY:** | Director, Legal Services, Head, Freedom of Information and Protection of Privacy | **Date:** **April 6, 2015** |
| | **APPROVED BY:** | Deputy City Manager, Head, Freedom of Information and Protection of Privacy | **Date:** **April 6, 2015** |
| * Note: Changes to the Freedom of Information and Protection of Privacy By-law in 2017 reduced the City's "Heads" from the three in the original approvals to the City Manager | **APPROVED BY:** | City Manager | **Date:** **September 22, 2021** |

**Next review date** **9/22/2023**