2026

FWC26 Situational Awareness Common Program

PRIVACY IMPACT ASSESSMENT

CITY OF VANCOUVER AND VANCOUVER POLICE DEPARTMENT

EXECUTIVE SUMMARY

Purpose

This Privacy Impact Assessment (PIA) evaluates the privacy implications of a time limited, common safety and security program supporting Vancouver's hosting of the FIFA Men's World Cup 2026. The Common Program enables coordinated situational awareness, incident response, and operational decision-making during a high-profile international event involving large crowds, dignitaries, and critical infrastructure in a National Terrorism Threat Level currently set at Medium.

Overview of the Common Program

The Common Program establishes a shared camera network and video management capability deployed across six defined zones in the City of Vancouver for the sole purpose of event safety, security, and operational coordination. It is explicitly not a generalized surveillance or intelligence gathering program.

The Camera System is designed for situational awareness, supporting real time monitoring and coordinated response to emerging risks. Recorded footage is reviewed only in response to a defined operational or investigative trigger and is subject to strict access, retention, and audit controls. The Common Program is temporary, with defined activation, decommissioning, and disposal timelines tied to the event window.

Governance and Participating Public Bodies

The Common Program is governed jointly by the City of Vancouver and the Vancouver Police Department (VPD), as Governance Partners, who are jointly responsible for determining the purpose, scope and parameters of the program. A limited number of Operational Partners (municipal, provincial, federal, and contracted service providers) may receive information on an as needed basis only to support safety, emergency management, transportation, infrastructure protection, and event operations. Operational Partners do not have governance authority and may not independently retain, repurpose, or expand the use of information.

All participation in the Common Program is governed by a common program governance and legal framework, which clearly distinguishes governance roles from operational access and establishes accountability, disclosure limits, and compliance obligations.

Privacy Risks and Mitigation

The PIA identifies elevated but manageable privacy risks, inherent to the temporary use of camera infrastructure in public spaces and the coordination of multiple partners.

Key risks include:

- Over-collection of personal information through video monitoring in public and semi-public environments
- Risk of function creep or unauthorized expansion of analytics

- Unauthorized access or misuse of information, including inconsistent practices across Participant Organizations in data access, breach reporting, and compliance with program obligations.
- Transparency and public perception risks associated with situational awareness technologies

These risks are mitigated through strong, layered controls, including:

- A clearly defined, time limited purpose tied to event safety and security
- Data minimization through controlled camera placement and limited analytics
- Explicit prohibition of facial recognition, and automated decision-making
- Role based access controls, audit logging, and restricted export functionality
- Defined retention limits with secure, verifiable disposal
- Mandatory privacy and security training for authorized users of the Camera System
- Clear public notice through signage and public facing materials

Residual risks are assessed as proportionate to the public safety objectives and acceptable given the safeguards in place.

Key Conclusions and Conditions

The PIA concludes that the program is lawfully authorized, necessary, and proportionate under the *Freedom of Information and Protection of Privacy Act* and is aligned with the OIPC's public sector surveillance guidelines.

Governance Participant approval and operation of the Common Program are contingent on:

- Final execution of the Common Program Agreement clearly defining governance and operational roles
- Full implementation of access controls, audit logging, and disclosure limitations
- Deployment of standardized collection notices and transparency materials before activation
- Enforcement of Common Program retention limits, secure disposal, and Camera System decommissioning at program end
- Completion of mandatory training for all Common Program Participant Organizations personnel
- Ongoing engagement with the Office of the Information and Privacy Commissioner for British Columbia (OIPC)
- Completion of an audit to ensure camera placement and system settings meet the requirements set out in this PIA.

Subject to these conditions, the Governance Participants are satisfied that the program's privacy risks are considered manageable and justified in light of the significant public safety and operational demands of hosting a major international event.

TABLE OF CONTENTS

PART 1 – PROGRAM OVERVIEW AND SCOPE

1.1 Program Objective and Description

The City of Vancouver (the "City") and the Vancouver Police Department ("VPD") have established a Common Program within the meaning of Schedule 1 of the Freedom of Information and Protection of Privacy Act ("FIPPA").

The Common Program is the coordinated delivery of real-time situational awareness to support public safety, operational coordination, and emergency response during the FIFA Men's World Cup in Vancouver, British Columbia ("FWC26"), through the shared operation of a temporary camera network and associated video management and analytics capabilities described in this PIA.

The Common Program is distinct from the City's and VPD's ordinary operations. It is established solely for the duration of FWC26 and is limited to the activities described in this PIA.

FWC26 is one of the highest-profile global sporting events, drawing significant international attention, dignitaries, athletes, and hundreds of thousands of spectators. The risk environment is elevated across multiple domains, including terrorism, public disorder, cyber threats, and infrastructure vulnerabilities. This is due to the symbolic significance, concentration of high-value targets, and global broadcast reach of the event. FWC26 is expected to bring approximately 350,000 people into the City of Vancouver for festivities.

As one of two selected Canadian cities, the City of Vancouver is scheduled to host seven soccer matches and associated cultural, social, and public events across designated venues and sites in the City. A core requirement for hosting an international sporting event of this scale is the coordinated delivery of public safety, and security, situational awareness, and emergency response services. The Common Program enables efficient communication and coordination during this time limited medium risk event. Further evidence of the event risk environment is addressed in Part 10 of this PIA.

The City has the following legal, contractual and operational responsibilities as a host city:

- event and property management within City managed spaces and responsibilities as the host jurisdiction;
- emergency management, including the assessment and mitigation of risks related to hazards and the detection and coordination of emergencies;
- street use and traffic management;
- public health and sanitation; and
- crowd and noise control, including safe pedestrian flow, barricades and traffic diversions, traffic signal adjustments, lighting, signage, and accessibility, creation and clearance of emergency evacuation routes, and safety inspections for stages, fan zones, and temporary venues.

On a broader scale, the City is also responsible for managing overcrowding in entertainment districts, ensuring emergency access routes remain open, and coordinating public communications in affected neighbourhoods.

The VPD leads policing within Vancouver as the municipal police service and primary police of jurisdiction. Other law enforcement partners coordinate with VPD within their respective jurisdictions. For clarity, security companies contracted by the City operate under the direction of the City and are not law enforcement. VPD is responsible for the following:

- enforcing federal and provincial statutes, including the *Criminal Code* and the *Liquor Control and Licensing Act*;
- coordinating with federal agencies, such as the Royal Canadian Mounted Police, Canadian Security Intelligence Service, and Canadian Border Services Agency as required, including the integration of intelligence from provincial and federal partners;
- responding to disturbances, fights, or disorderly conduct;
- deploying specialized units (mounted, marine, tactical, K9) as needed
- coordinating close protection, motorcades, and secure routes, often alongside federal agencies, for athletes, officials, and VIPs;
- protecting critical infrastructure; and
- responsibilities under the *Police Act.*

1.1.1 Camera Network Timeline

The City is installing a temporary camera network as the technical foundation of the Common Program. Following installation and configuration, all cameras will remain active with privacy filters applied to the live feed to prevent any footage from being recorded. A limited number of cameras will be activated without privacy filters for the purpose of a joint exercise on April 16, 2026, following which the privacy filters will be reinstated, except as required for intermittent field testing. The camera network will operate from June 7 to July 19, 2026, following which the cameras will be turned off, and the temporary network will be fully decommissioned and removed.

1.2 Statutory and Policy Framework

The primary legislative authority for the collection, use, and disclosure of personal information under the Common Program is FIPPA. The Common Program has also been designed in accordance with the Office of the Information and Privacy Commissioner for British Columbia's public sector surveillance guidelines.

The City and the VPD are the only two Governance Partners for the Common Program. Each Governance Partner retains responsibility for authorizing disclosure of program information to its respective Operational Partners (as set out in Section 1.3.1). A total of 23 additional public bodies, federal departments, or agencies that may receive personal information from the Common Program as Operational Partners on an as-needed basis.

Operational Partners access to program information is by observation only within the City's Emergency Operations Centre (EOC), the VPD's Command Centre FIFA (VCCF), VPD Operations Command Centre (OCC) or a local zone control centre. Operational Partners do not have the ability to independently retain information gathered from the camera network without knowledge and approval from a Governance Partner.

Over and above the authorities created via the common program, the VPD possesses authority to collect, use, and disclose personal information for law enforcement purposes under the *Police Act*.

The City and VPD will operate the Common Program on a hub and spoke model, with the City and the VPD acting as the primary custodians of the information collected through the Common Program. Personal information may then be disclosed to their respective Operational Partners within their respective spheres of influence, as is required for the operation of the Common Program. While the Governance Partner's disclosure to Operational Partners will be under the authority of the Common Program's governing legal framework, each Operational Partner's authority to collect personal information for a necessary purpose is determined by their existing enabling legislation or statutory authority.

1.3 Program Governance Model

The Common Program is constituted as a common or integrated program via agreement, in accordance with section 12 of the FIPPA Regulation. The Common Program is operated by designated senior leads who are responsible for overseeing the management of their respective responsibilities from City and the VPD. The overall program lead for the City is the Deputy City Manager and the lead for the VPD is the Deputy Chief for Strategy & Innovation.

Each Governance Partner retains responsibility for authorizing disclosure of program information to its respective Operational Partners (as set out below in Section 1.3.1) only where necessary to support delivery of the Program.

The Common Program operates on a hub and spoke model. The Governance Partners form the centre of the hub, gathering and providing the information necessary to operationalize the safety and security of the event. Each of the Governance Partners are responsible for communicating information to, and coordinating with, their respective sphere of influence of agencies should there be an event that requires services.

The City and the VPD are each responsible for the following secondary recipients of Common Program information:

1.3.1 Governance Partner #1

City of Vancouver (the City) including Vancouver Fire and Rescue Services (VFRS): FIPPA and *Vancouver Charter*

1.3.1.2 Operational Partners:

- **UBC**: FIPPA and *University Act*
- **PNE**: FIPPA and *Pacific National Exhibition Act*
- **FIFA**: FIPPA
- **Ministry of Emergency Management and Climate Readiness:** FIPPA and *Emergency Disaster Management Act*
- **Health Emergency Management BC**: FIPPA and *Health Emergency Management BC Act* - representative could be from the Ministry, VCH, FHA, or PHSA
- **Metro Vancouver Regional District**, through its Metro Vancouver Emergency Management program, FIPPA and *Local Government Act*

- **City of Richmond** through its Emergency Management Program, FIPPA and *Community Charter*
- **Public Safety Canada**: *Emergency Management Act* (federal), *Safe Streets and Communities Act*
- **Ministry of Tourism, Arts, Culture, and Sport:** FIPPA and *Athletic Commissioner Act*
- **Environment and Climate Change Canada**: *Canadian Environmental Protection Act*
- **Translink,** via BC Regional Transit Company and Coast Mountain Bus Company: FIPPA and *South Coast British Columbia Transportation Authority Act*
- **BC Hydro**: FIPPA and *Hydro and Power Authority Act*
- **Port of Vancouver:** *National Harbours Board Act*
- **FortisBC**

1.3.2 Governance Partner #2:

Vancouver Policy Department (VPD): FIPPA, *Police Act*

1.3.2.1 Operational Partners:

- **Metro Vancouver Transit Police**: FIPPA and *Police Act*
- **BC Emergency Health Services (ambulance):** FIPPA and *Emergency Health Services Act*
- **E-Comm:** FIPPA and *Emergency Communications Corporations Act*
- **Vancouver International Airport (YVR)**: *Aeronautics Act* and *Vancouver International Airport Zoning Regulations*
- **Royal Canadian Mounted Police**: *Police Act* and *Royal Canadian Mounted Police Act*

A further breakdown of each party and their role is found in section 2.2.

For the purposes of this PIA, Operational Partners have no role or influence in the governance of the Common Program. No party other than the City and VPD has any control over the infrastructure, placement of cameras, use of analytics, or any other governance aspect of the Common Program. The Operational Partners will receive information on an as-needed basis from the applicable Governance Partner, where required to be present or assist in coordinating a response to a situation or event. The City and VPD program leads have final decision-making authority on the use and disclosure of personal information resulting from the Program.

1.4 Scope of This PIA

This PIA applies to the Common Program as described in Section 1. The responsibilities and activities set out above in this Section establish the operational necessity of the Common Program, pursuant to FIPPA section 26, as well as justifying the data minimization and proportionality of the technological response for the Program.

The PIA also addresses the technology the City and VPD are deploying for the Common Program. This includes a video management platform, video analytics, and camera specifications, as well as how the information is governed, what information will be collected, used, and disclosed, and how the information will be disclosed to secondary parties on a need-to-know basis.

The six distinct zones are:

- Killarney Training Facility;
- UBC National Soccer Development Centre;
- FanFest at the PNE / Hastings Park;
- Event approach near BC Place;
- Hotel zone, covering the exterior of official hotels, Jack Poole Plaza, and Vancouver Convention Centre; and
- Entertainment zones, covering Granville Street and Commercial Drive.

Each of these zones uses the same common data infrastructure as set out in this PIA. However, further details about each zone are set out in Annex A.

The necessity and proportionality of the Program are assessed in Part 4 of this PIA. Activities and systems outside the scope of this assessment are described in Section 1.5 below.

1.5 Out-of-Scope Activities

This PIA applies solely to the Common Program and Camera System established for FWC26. It does not apply to any other FWC26 activities, or to any other City or VPD programs, operations or activities. This PIA does not extend to any future use of the camera network, and the use of facial recognition technologies is not within the scope of this PIA.

Further, this PIA does not contemplate pre-existing CCTV networks used for traffic, building security, or other reasons by the City, VPD, or other partners and agencies. These camera networks are not connected to, and do not feed into, the Camera System addressed in this PIA.

This PIA does not contemplate the standard operational requirements of the VPD, including any independent special operations the VPD may conduct in connection with FWC26. Rather, this PIA is a supplement to the VPD's existing authorities for extraordinary circumstances presented by FWC26.

PART 2 – PROGRAM STRUCTURE AND PARTICIPATION MODEL

2.1 Common Program Agreement

The Common Program Agreement (CPA) is initially established between the Governance Partners: the City and the VPD. The CPA outlines the governance roles of the City and the VPD, and other Operational Partners, as well as responsibilities, and operational arrangements for the Program.

Additional Operational Partners will sign-on as data recipients. The CPA will also act as, and contain all the necessary elements, of an information sharing agreement. This will ensure common knowledge and understanding of responsibilities among all parties.

2.2 Membership

2.2.1 Governance Partners

The City and the VPD are the two founding Governance Partners to this CPA. While the VPD and City do not anticipate requiring future Governance Partners, it is prudent to establish procedures for potential future alterations.

Should an additional Governance Partner be required, the City and VPD must agree and jointly extend an offer to join the program as a governance partner. This new partner would need to sign-off on all the provisions of this PIA and sign off on the CPA. Should this occur, their unique role and requirements will be documented in the annexes.

2.2.2 Operational Partners

All additional participants in the Common Program are limited Operational Partners who receive information but do not make governance decisions. No Operational Partner has any control over the placement of the cameras, defining what analytics get run, and the right to independently demand the export of footage for their purpose. The City and VPD do not see a requirement for any other public body, agency, or federal department to perform these functions.

Operational Partners who will be in the Emergency Operations Centre or VPD Ops Centre but are not a Governance Partner will be required to sign onto the CPA but not the PIA. These public bodies and organizations can be found in section 1.3 above. Should additional public bodies or organizations be required, the City or the VPD would need to extend the offer to sign onto the CPA and notify the other party through a modification to the PIA.

2.3 Program Camera Zones

There are six identified zones for the deployment of cameras. Each of these zones function similarly on the ground, with a local command staffed by specially trained CCTV operators. This allows for a rapid response to any situation, should one arise. Each zone differs is in what it is protecting and how many people may be involved. It should be noted that zones 5 and 6 (hotel and entertainment) will be aggregated into the ground command of the Last Mile zone.

2.3.1 Killarney Training Facility

This zone, located in Killarney Park in South Vancouver, contains 24 cameras and is one of two locations where teams will train before their matches at BC Place. This location is not open to the public during FWC26 and will be patrolled s.15 s.15 s.15

2.3.2 UBC National Soccer Training Centre

This location is used as a Team Base Camp training facility during the Group Stage of FWC26. This is also an alternative training zone for teams prior to their matches at BC Place. This zone will have 14 cameras and is not open to the public during FWC26. s.15 s.15

2.3.3 FanFest at the PNE

This zone is the Vancouver FIFA Fan Festival site located at Hastings Park on the Pacific National Exhibition (PNE) grounds. This zone includes festival programming and amenities such as food and beverage service (including beer garden(s)) and large screens for live match viewing. The site operates on selected dates during the tournament window (June 11–July 19, 2026), with proposed daily hours varying by day. It is important to note that these days are not limited to just Vancouver match days. It will contain 43 cameras and is located on the site of the Pacific National Exhibition (PNE). It is anticipated that this zone will hold 25,000 people plus staff during games, regardless of location in North America.

2.3.4 Event approach near BC Place (Last Mile)

This zone covers the event approach near BC Place (Last Mile), which is a designated, managed network of pedestrian corridors and adjacent public spaces surrounding BC Place Stadium that connects spectator arrival routes (including nearby transit) to the primary Pedestrian Screening Areas (PSAs) and the Outer Security Perimeter (OSP) for matchday ingress, and supports post-match egress and dispersal back toward transit and other destinations.

This zone will hold just under 55,000 ticket holders prior to, and at the conclusion of, matches at BC Place. In addition to the cameras, up to s.15 22(3)(b) in this zone. s.15 s.15

2.3.5 Hotel zone

This zone includes the official hotels of the s.15 s.15 s.15 These hotels will be hosting s.15 visiting teams playing games within the City. s.15 In addition to the cameras, s.15 .

2.3.6 Entertainment zone

This zone covers Granville Street and Commercial Drive, both of which are expected to swell in numbers during the event. Both streets are expected to experience significant increases in pedestrian traffic during FWC26. Granville Street is a popular entertainment district with numerous venues for fans to gather and watch the games. Granville Street will also be closed to vehicle traffic, making it a densely packed pedestrian zone.

Similarly, Commercial Drive is home to diverse communities with a strong connection to the sport. It is a frequent area for the City to see a large influx of people during soccer events in the City and will likely see significant activity, especially if internationally popular teams participate in matches in Vancouver.

This zone will be patrolled by the VPD.

Collectively, the Last Mile, along with the Hotel zone and Entertainment zone will contain approximately 110 cameras.

PART 3 – INFORMATION AND DATA ARCHITECTURE

3.1 Information Types and Personal Information Inventory

The Common Program processes both raw video footage and derived information generated through analytics. For clarity and regulatory transparency, the Common Program distinguishes between primary and secondary information types as follows:

3.1.1 Primary Information (Raw Video Footage)

The majority of information discussed in this PIA involves video footage captured from the Camera System's 190* cameras placed in the six zones around the City. This includes:

- Video recordings captured by fixed or mobile cameras deployed in program zones
- Live video streams viewed by authorized personnel for situational awareness
- Still images or clips exported from video footage for authorized purposes and noted in audit logs, along with file and/or investigation numbers
- Event Alerts (as defined in Appendix A), being notifications generated by the video analytics component of the Camera System when a pre-defined operational rule or condition is met, which may include a still image or short video clip derived from the camera footage and made available through the Common Operating Platform (COP) for situational awareness, such as a car parked in a zone that has been blocked off or the trespass of a boundary.
- Raw video footage constitutes personal information where individuals are identifiable or reasonably identifiable.

3.1.2 Derived Information (Analytics Metadata)

As with most digital systems, the video management platform will generate analytic metadata and access logs based on what is happening in the system. Further metadata will be accumulated from the use of the analytics overlay. In all, the derived information should include:

- System-generated metadata describing detected objects, movements, counts, and events
- Attribute-based descriptors (e.g., direction of travel, speed, dwell time, object category)
- Aggregated statistical outputs such as counts, heat maps, and trend reports

3.1.3 Identifiable information

While the City and VPD are deploying cameras, the intention is to monitor more for situational awareness rather than intended identification, unless an investigation is required. However, due to the location and quality of the cameras, it is unlikely that personal information will be wholly avoided. To this end, it is likely that the camera network will capture:

- Direct visual identifiers, such as distinguishing characteristics and clothing;

- Quasi-identifiers, such as height, approximate age, body type, clothing, accessories, and movement pattern (direction);
- Temporal location data: time and date of recording, combined with the person's presence and location of the camera identified;
- Inferred data: object and/or behavioural inferences, such as mood based on expression, activities such as loitering and queuing, and crowd formation. Note that behavioural inferences are done solely by observation and not using video analytics.

3.2 Information Classification

All information processed under the Common Program is classified in accordance with public-sector information classification standards. Raw video footage and derived analytics metadata are classified at a minimum as Protected Personal Information and are subject to equivalent or higher safeguards.

Aggregated outputs that are de-identified and used solely for high-level statistical reporting may be classified at a lower sensitivity level only where re-identification risk has been assessed and mitigated.

3.3 Data Sources

A complex, integrated security plan includes many sources of information to ensure safety and stability of an event. These include:

3.3.1 Direct Collection Sources

- Cameras deployed in public or controlled environments within program zones
- Visual confirmation of events
- Witness statements, where necessary
- Observation by patrols and security guards

3.3.2 Indirect and System-Generated Sources

- Metadata and event data generated by the analytics platform based on analysis of authorized video feeds
- Event Alerts
- Audit logs of activity

3.4 Data Flow Summary

At a high level, data flows operate as follows:

1 Cameras capture video footage within defined zones and transmit footage to the VMS.
2 Authorized video streams or recordings are processed by the analytics overlay.
3 The VMS streams the footage to the local security station, and the version with analytics to the Emergency Operations Centre, and VPD headquarters.
4 The VMS stores footage in accordance with program retention and access controls.
5 The analytics overlay generates metadata, alerts, and analytical outputs

6 Authorized users access video and analytics outputs through controlled interfaces

All data flows remain subject to centralized access controls, audit logging, and governance, as described in the remainder of this PIA. A flow diagram is included in section 5.1.

3.5 System Components and Deployment Architecture

3.5.1 Service Providers and Sub-Processors

The Common Program relies on a defined set of core technology vendors and supporting sub-processors to enable collection, transmission, processing, and operational coordination. These entities provide infrastructure and technical capabilities only, and do not exercise independent decision-making authority over the collection, use, or disclosure of personal information.

The table of Service Providers and Sub-processors is as follows:

Service Provider	Role
TELUS	s.15
Datavalet	
Paladin Technologies (Bosch)	
Cisco	
Fortinet	
Axon	
Dell	
Digi	
s.15	
Industrio	
Jasper	
Paladin Security	
Securiguard	
GuardTek	
Universal Traffic	

All service providers operate under contractual agreements with the City that include privacy, security, and use limitation requirements, and are subject to program-level governance controls. The use of sub-processors is limited, disclosed, and contractually constrained, and does not expand the authorized purposes of the program.

3.5.2 Camera Deployment Overview

The Common Program utilizes a defined set of camera types deployed across designated zones to support situational awareness, safety, and operational coordination during the event. Camera deployment has been designed to align with the principles of necessity, proportionality, and data minimization, with configurations tailored to the specific characteristics and risk profiles of each zone.

Cameras are overt, fixed, and non-targeted, and are positioned to capture broad environmental context rather than detailed observation of individuals. Deployment is limited to areas where

monitoring is required to support program objectives, such as entrances and exits, high-traffic corridors, and event-related operational zones. Cameras are not installed in locations where individuals would be expected to have a reasonable expectation of privacy, such as interior private spaces. The types of cameras used and their general capabilities are described below.

The camera deployment approach reflects a controlled and purpose-specific implementation, in which each camera type is selected and configured to support defined operational needs without expanding the scope of collection beyond what is necessary. Camera placement and configuration are subject to ongoing review and adjustment to ensure alignment with privacy requirements and program objectives.

While camera technologies inherently involve the capture of individuals within the field of view, the Common Program mitigates associated privacy risks through non-targeted use, restricted functionality, limited retention, and strong governance controls over access and disclosure. Deployment is time-limited to the duration of the event, with all equipment and associated data handling practices subject to established decommissioning requirements.

PART 4 – PURPOSE, NECESSITY, AND PROPORTIONALITY

This section reviews the necessary test set out in the BC OIPC's public sector surveillance guidelines, as well as the proportionality of the program, as deemed necessary by the common program partners.

4.1 Definition of the program or activity

A part of the requirement for hosting any international sporting event is the safety and security of citizens, visitors, players, and dignitaries. As a host city for FWC26, the City has agreed to develop and implement a safety and security concept that it will operationalize in collaboration with the VPD

The safety and security concept forms part of the City and VPD's command, control, coordination, and communication structure (C4), a framework that connects all operational partners, including operational venues, sites, and participating agencies to support coordinated safety and security delivery during FWC26. This reference to the C4 structure is provided for context only. This PIA is limited to the temporary camera network and associated video management and analytics capabilities described herein.

The core responsibilities of this program are split between the City and the VPD. As such, the City and VPD have agreed to create a common program to enable efficient communication and coordination during this medium-high-risk event.

The Common Program involves the deployment of an event-based Camera System for defined public safety and security purposes. While any camera network that captures identifiable individuals may be characterized in a broad sense as surveillance, the Common Program is not designed or operated as a generalized or intelligence-led surveillance network. In this context, "surveillance" typically refers to the systematic, directed, and sustained monitoring of identifiable individuals or groups for behavioural analysis, profiling, or control. That is not the primary purpose or design of the Common Program.

Rather, the Camera System is configured for situational awareness, meaning the real-time monitoring of defined environments to detect emerging safety risks, coordinate operational response, and support immediate incident management. The system is not designed or configured for ongoing monitoring of specific individuals, behavioural profiling, or persistent cross-camera tracking across time or location. The review of recorded footage occurs only in response to a documented operational, safety, or investigative trigger, and is subject to defined access controls, role-based permissions, audit logging, and time-limited retention requirements.

The Program is multifaceted, encompassing the deployment of cameras to assist City staff and the VPD in managing large scale event crowds across multiple locations concurrently, who themselves are navigating across multiple venues. It also assists law enforcement in efficiently managing the strategic deployment of resources to the event, while allowing them the ability to still respond to standard operational requirements elsewhere.

4.2 Program or activity's mandate under the public body

While both the City and the VPD will have equal access to the Common Program's Camera System, each Governance Partners only use the cameras for activities within its respective jurisdiction, recognizing that there is some overlap.

4.2.1 The City

The City relies upon the *Vancouver Charter* for its mandate. Specific sections include section 145, which empower the City to engage in any commercial, industrial, or business undertaking and section 189 which empowers City Council ("Council") to provide for the good rule and government of the City. Further, section 199 of the Charter empowers Council to do "all such things as are incidental or conducive to the exercise of the allotted powers." This language implicitly empowers the City to enter into agreements to operate festival venues and host major sporting events, accompanied by the exercise of any and all duties required to ensure those commercial or business undertakings are successful.

Exercise of municipal powers is subject to review on the reasonableness standard, *1193652 B.C. Ltd. v. New Westminster (City)*, 2021 BCCA 176, at paras. 59 to 61. The authority to enter into a specific area does not require a specific authority be found in the Vancouver Charter. It is sufficient for the City to determine that the various elements of the Vancouver Charter when read together provide the requisite authority. This is in accordance with the "broad and purposive" approach to the interpretation of municipal powers, which was first articulated by Justice McLachlin, as she then was, in dissent, in *Shell Canada Products Ltd. v. Vancouver (City)*, [1994] 1 S.C.R. 231, and has since been adopted by the Supreme Court of Canada in multiple decisions. At paragraph 27 of her dissent, Justice McLachlin expressly notes the City's role in promoting safety as one of the purposes of municipal legislation.

Read together, the provisions of the Vancouver Charter establish a clear mandate for the City to:

- Conduct event and property management as the host and property owner (*Vancouver Charter* ss.145 and 199);
- emergency management, including the assessment and mitigation of risks related to hazards and the creation and coordination of emergencies (peace, order, and good government related to the above event);
- street use and traffic management (*Vancouver Charter* s. 290 and 291);
- public health and sanitation (*Vancouver Charter* ss. 145, 291(j), and 302); and
- crowd and noise control, including safe pedestrian flow, barricades and traffic diversions, traffic signal adjustments, lighting, signage, and accessibility, creation and clearance of emergency evacuation routes, and safety inspections for stages, fan zones, and temporary venues (*Vancouver Charter* s. 290 and 291 – protection of streets, in relation to streets and other matters).

4.2.2 The VPD

The VPD relies upon its law enforcement authorities under the *Freedom of Information and Protection of Privacy Act* as well as the *Police Act* for its authorization to engage in the common program. Specifically, it is noted that this is a time-limited event during which there is a significant influx of visitors and activity in select regions of the City, as defined by the zones.

From a law enforcement perspective, the following activities clearly fall under the jurisdiction of the VPD:

- enforcing federal and provincial statutes, including the *Criminal Code* and the *Liquor Control and Licensing Act*;
- coordinating with federal agencies, such as the RCMP, CSIS, and CBSA as required, including the integration of intelligence from provincial and federal partners;
- responding to disturbances, fights, or disorderly conduct;
- deploying specialized units (mounted, marine, tactical, K9) as needed
- coordinating close protection, motorcades, and secure routes, often alongside federal agencies, for athletes, officials, and VIPs; and
- protecting critical infrastructure.

4.3 Information directly related to the program or activity

The deployment of the Common Program cameras is directly related to the program activities set out in section 4.1 and 4.2 above in the following ways:

4.3.1 Enabling a rapid response

This is the primary advantage to using cameras to supplement and assist individuals operating on the ground. CCTV in a live-monitored environment allows a higher vantage view for coordination, allowing first responders to more quickly navigate to individuals in distress within crowded environments, understand what is happening on the ground, and coordinate the correct types of response. Personal information in cases of medical distress is vital for a timely response.

4.3.2 Managing access and protecting restricted areas

This is one of the primary advantages to the deployment of analytics. There are a finite number of resources that the City and VPD can deploy to manage large crowds. The deployment of cameras with analytics can trigger alerts and assist in the deployment of resources should boundaries be violated.

4.3.3 Identifying threats and supporting investigations

This primarily relates to the VPD. The use of cameras, with select recording only occurring when something goes wrong, allows law enforcement to reconstruct events, identify suspects and witnesses, verify timelines, and provide evidence for legal proceedings. However, from a broader perspective, it would also enable the City or VPD to identify crowd movement patterns and/or respond quickly when someone is in danger. Without identifiable information, the cameras effectively become motion detectors only.

4.4 Necessity

Largescale events of this nature require coordinated situational awareness across multiple agencies, including the City, VPD, private security providers, and other partners. While personnel remain essential to event operations, no number of on the ground staff can provide the continuous, wide area visibility needed to monitor dynamic crowd movement, identify emerging safety issues and support timely deployment decisions. CCTV is therefore used as a necessary supplement, consistent with common practice for major events in urban environments.

The purpose of CCTV in this context is not criminal surveillance or deterrence, but real time crowd and event management. Cameras provide a vantage point that enables incident detection, crowd flow monitoring, and rapid coordination among response teams. This capability cannot be achieved through personnel alone, regardless of staffing levels, because physical presence is inherently limited by line of sight, crowd density, and the geographic scale of the event footprint.

The Camera System is designed and deployed in accordance with necessity and proportionality principles under applicable privacy legislation. Camera placement is limited to areas where situational awareness is operationally required, and the configuration minimizes the collection and downstream use of personal information beyond what is necessary to meet defined public safety objectives.

As noted by Commissioner Loukidelis in Order F0710, “necessary” does not require a measure to be indispensable, but it must be more than merely convenient. In this case, CCTV provides an operational capability that is functionally distinct from what personnel can offer and is widely recognized as a standard component of major event safety planning. Its use is therefore justified as a necessary and proportionate tool to support public safety, emergency response, and effective resource deployment.

PART 5 – COLLECTION, USE, AND DISCLOSURE OF PERSONAL INFORMATION

5.1 Program-Level Data Flows

The Common Program relies on a hub-and-spoke data flow model, with the City's EOC operating as the central hub for video footage collection. The EOC then provides authorized access to video footage via the VMS to VPD Ops Centre for VPD's command with law enforcement. The City's EOC also provides authorized access via the VMS to local security stations established in Zones 1-4. A visual flow diagram of the hub-and-spoke model can be found in Annex C.

The City and VPD are the central data collectors and governance operators under the Common Program, acting as the hub, and disclosing relevant data outward to Operational Partners on an as-needed basis. The Camera System supporting the Common Program operates through a shared technical environment and coordinated operational workflows. Further information about the technical systems supporting the Common Program, including about the VMS and analytics platform, is set out in Part 6 of this PIA.

At a program level, the flow of information occurs in six primary stages.

5.1.1 Visual Collection

Video cameras deployed within the designated Common Program zones capture visual information about the surrounding environment, which may include images of identifiable individuals, vehicles, and activities occurring in public spaces. The cameras transmit live video feeds through the Camera System's communications network to the central Video Management System (VMS), and relevant alerts are pushed into the Common Operating Platform.

5.1.2 Ingestion and Management within the VMS

Live video streams are ingested into the VMS, which serves as the system of record for all video footage collected under the Common Program, managing its recording, indexing, storage, analytics and retrieval. This footage can then be accessed and recalled by Governance Partner authorized CCTV operators within the City EOC and VPD Command Centre via VMS controlled interfaces. User access and retrieval of video footage within the VMS is logged for audit purposes.

Video data is stored within the Common Program's designated on-premises data infrastructure, located at the secure data centre described in Section 7.

5.1.3 Analytics Processing Platform s.15

Video feeds may be processed by the analytics platform s.15 to generate analytical outputs intended to support operational awareness. These video analytics may identify patterns, objects, or events within video footage and produce outputs such as:

- Event Alerts
- Searchable metadata
- Activity summaries or statistical insights

s.15 processes video footage already collected through the VMS and generates derived information within the scope of the authorized purpose of the Program. The analytic outputs do not introduce new collection points. Searchable metadata and activity summaries or statistical insights are accessible to the authorized City and VPD operators within the VMS and s.15 environment.

Access to analytics outputs is role-based and limited to operational need, as further described in section 7.4.1 The outputs are used to assist authorized users in locating relevant video footage or understanding situational developments.

Video footage and derived analytics information remain within the VMS and analytics environment and are not stored within the Common Operating Platform.

5.1.4 Operational Access and Use

Authorized personnel from Governance Partners and their service providers may access the Camera System only through secure viewing stations located within designated operational environments, being either secured PC workstations or laptops within the City EOC or VPD Ops Centre, or local zone security offices using VMS-controlled access mechanisms.

5.1.5 Disclosure and Information Sharing

At a program level, personal information collected under the Program is disclosed only where authorized by FIPPA and consistent with the governance arrangements set out in this PIA. The substantive disclosure rules, permitted disclosure scenarios, and applicable FIPPA authorities are set out in Section 5.5 of this PIA.

Examples include:

- Disclosure to law enforcement where authorized for investigative purposes
- Sharing visual information among Participant Organizations to coordinate operational responses
- Provision of records in response to access-to-information requests

The Common Program does not target specific individuals. Information about specific individuals will only be disclosed by the VPD to law enforcement partners if there is a specific investigation by one of its partners.

Analytics outputs are not disclosed externally as standalone datasets. Any disclosure relies on the underlying video footage and applicable legal authority.

5.1.6 Retention and Disposition

Video footage and related information are retained according to the retention schedules established for the Program and the statutory obligations of Participant Organizations.

Once the retention period has expired, footage is securely deleted or overwritten within the system unless it has been preserved for an authorized purpose such as an investigation, legal proceeding, or access request. The full retention and disposition framework is set out in Part 9 of this PIA.

5.2 Legal Authority Mapping

Personal information collected through the program may be used for the following authorized purposes:

- Monitoring and maintaining safety and security within Common Program zones;
- Supporting incident detection, response, and investigation;
- Facilitating efficient review of video footage through search and analytics;
- Producing aggregated, non-identifying statistics for operational planning and evaluation

Uses must align with program objectives and partner-specific authorities as documented in this PIA.

The table below maps each Common Program activity by type of collection, use, or disclosure to the applicable FIPPA authority, and provides the legal foundation for the collection, use, and disclosure framework set out in sections 5.3, 5.4, and 5.5 respectively.

Activity	**Type**	**FIPPA Authority**	**Other Authority (if applicable)**
Collection personal information for an investigation where a penalty or sanction may be imposed	Collection	s.26(b) - collection for the purpose of law enforcement	
Collect personal information directly from individuals for program administration	Collection	s.26(c) – collection relates directly to and is necessary for an operating program or activity of the public body	
Collection for deidentification and subsequent use for evaluation of the event and planning for future major events.	Collection	s.26(e) – collection relates to planning and evaluating a program or activity	
Collection of personal information directly from individuals during the event	Collection	s.26(g) – collection by observation at a presentation, ceremony, performance, sports meet or similar event	
Use personal information for the purpose for which it was obtained	Use	s.32(a) – use for the purpose for which information was obtained or compiled	

Use personal information for the necessary operations of the common program	Use	s.32(c) – for a reason it may be disclosed under s.33(2)(k)	
Disclosure to program partners for the participation in and operation of the common program	Disclosure	s.33(2)(k) - disclosure for the necessary delivery of a common program	
Disclose personal information to another public body for program administration	Disclosure	s.33(2)(d) – disclosure for purposes consistent with the program	
Disclose personal information for law enforcement purposes	Disclosure	s.33(3)(d) – disclosure for law enforcement	*Police Act / Criminal Code*
Disclose personal information necessary for performance of duties	Disclosure	s.33(2)(h) – disclosure necessary for performance of duties	
Disclose information to a service provider operating under contract	Disclosure	s.33(2)(t) and (v) – disclosure to service provider for program operations	
Disclose information where necessary to protect health or safety	Disclosure	s.33(2)(i) – disclosure to prevent or reduce risk of harm	
Share analytics outputs between governance participants	Disclosure	Not personal information if properly de-identified	
Provide aggregated program reporting	Use / Disclosure	Not personal information if properly de-identified	

5.3 Collection of Personal Information

Personal information is collected under the Program by the Governance Partners pursuant to the authorities set out in Section 5.2. Operational Partners may collect personal information through the operation of visual monitoring systems and through direct visual observation, within the scope of the Common Program.

Personal information collection may occur through:

1. Fixed camera systems installed at designated locations within the zones (see Annex A: Zone Specifics); and
2. Direct visual observation by Operational Participants operating within the scope the Common Program.

Collection is intended to support the operational objectives of the Program, including situational awareness, public safety coordination, operational management, and incident response and coordination across Program zones

Personal information collected through these methods may include:

- the visual image of identifiable individuals;
- clothing, physical characteristics, and observable behaviours;
- the presence, movement, or interaction of individuals within Common Program zones;
- time, location, and contextual information associated with recorded images or observations.

5.3.1 Collection by Operational Partners

Operational Partners may conduct visual observation where:

- the activity falls within the approved scope of the Common Program;
- the location has been approved by the Governance Partners (respective EOC and VPD Ops Centre);
- appropriate public notification signage is displayed; and
- personnel have received training regarding privacy obligations and Common Program policies.

Operational Partners do not have authority to determine or modify the scope of collection and must operate strictly within the parameters established by the Governance Partners. Further, Operational Partners do not independently expand the locations, duration, or technical capabilities of the collection systems.

5.3.2 Notice of Collection

Notice of collection will be provided through clearly visible signage placed in locations where camera monitoring or visual observation may occur.

The signage will read:

> "This area is temporarily under CCTV monitoring during the special event.
>
> By entering this zone, your personal information is collected under section 26(c) of the *Freedom of Information and Protection of Privacy Act* for the purpose of providing situational awareness and ensuring safety and security during the games.
>
> Your privacy is important to us. If you have any questions, please contact privacy@vancouver.ca."

A visual sample signage is included in Annex E.

5.3.3 Limitations on Collection

Collection is limited to what is reasonably necessary to support the purposes of the Common Program. Camera placement, camera angles, and observation practices are configured to avoid unnecessary or disproportionate collection of personal information.

The Governance Partners are making all reasonable efforts to avoid capturing images of areas where individuals would have a heightened expectation of privacy. The City will conduct an audit of the Camera System setup prior to activation to ensure the system meets the requirements of this PIA.

5.3.4 Prohibited Collection Activities

The following activities are expressly prohibited unless supported by lawful authority:

1. Audio recording through camera systems;
2. Facial recognition technology;
3. Automated identification, tracking, or profiling of individuals;
4. Collection within locations where individuals have a heightened expectation of privacy, including:
    - washrooms
    - private residences
    - change rooms
    - medical treatment areas
5. Collection for purposes unrelated to the Common Program;
6. The use of personal devices or unauthorized recording equipment for Common Program collection activities; and
7. The use of Camera Systems for monitoring individuals based solely on race, ethnicity, religion, political beliefs, or other protected characteristics.

Any proposed expansion of collection capabilities must be approved by the Governance Partners and may require an update to this PIA.

5.4 Use, Use Limitations, and Prohibitions

Personal information collected through camera systems or through visual observation conducted under the Common Program may be used by Participant Organizations solely for the purposes authorized under the Common Program Agreement and applicable legislation.

Authorized uses include:

1. Supporting situational awareness for the Common Program;
2. Assisting in the coordination and management of operational activities conducted by Participant Organizations;
3. Monitoring conditions within Common Program zones in order to support public safety, event operations, and operational decision-making;
4. Assisting personnel responsible for operational response by providing real-time visual context (“eyes-in-the-sky” situational awareness);
5. Supporting coordination between Participant Organizations where information is required to respond to incidents, manage operations, or address safety concerns;
6. Documenting incidents that occur within monitored Common Program zone locations;
7. System testing to ensure all components and features operate as expected; and
8. Supporting lawful investigations or operational reviews related to Common Program activities.

The use of personal information will remain directly connected to the operational purposes of the Common Program.

5.4.2 Use by Governance Partners

Governance Partners may use personal information derived from the Camera System for purposes including:

- oversight of Common Program operations;
- incident review and analysis;
- program administration and evaluation;
- application of limited, situational analytics to create alerts for human review;
- coordination between Participant Organizations; and
- compliance, accountability, and audit activities.

Governance Partners will ensure that any such use remains consistent with the purpose for which the information was collected.

5.4.3 Use by Operational Partners

Operational Partners may access or use personal information from the Camera System only where such access is necessary for the performance of their statutory functions and authorities or contractual obligations under the Common Program.

Operational Partners may use visual information to:

- communicate relevant situational information to personnel within their own organization;
- assist operational teams responding to incidents or safety concerns;
- provide real-time situational awareness to operational leadership; and
- support coordination between partner organizations involved in the Common Program.

Operational Partners may verbally relay relevant information observed through camera monitoring to authorized personnel within Participant Organizations where necessary to coordinate operational activities.

Operational Partners shall not obtain or retain, copy, or otherwise use personal information outside the scope of the Common Program without authorization from a Governance Partner.

5.4.4 Limitations on Use

Each Participant Organization will limit the use of personal information to what is reasonably necessary to support the purposes of the Common Program.

Personal information derived from the Camera System will not be used for purposes unrelated to the Common Program or outside the lawful authority of each relevant Participant Organizations.

The Governance Partners have implemented role-based access controls and operational procedures to prevent unauthorized or unnecessary use of Camera System information.

5.4.5 Prohibited Uses

The following uses of personal information collected through the Camera Systems or visual observation are expressly prohibited under the Common Program:

1. Facial Recognition Technology (FRT) technology.
2. Automated identification, tracking, or profiling of individuals.
3. Behavioural analytics designed to identify individuals or infer personal characteristics unrelated to the Common Program.
4. Monitoring individuals for purposes unrelated to operational Common Program activities.
5. Use of the Camera System for employee surveillance except where incidental observation occurs as part of the necessity to coordinate with the “eyes in the sky” coordination approach.
6. Commercial use of images or footage collected through the Common Program.
7. Use of identifiable camera footage for future training, demonstration, or media purposes unless personal information has been removed or de-identified.
8. Attempting to identify individuals captured in camera footage where such identification is not required for authorized operational purposes.

5.4.6 Technical and Contractual Controls

The Governance Partners have ensured that technical and contractual controls are in place to support compliance with the limitations described in this PIA. Details on the technical and contractual controls supporting compliance with the limitations of the Common Program are set out in Part 7 of this PIA.

5.4.7 Prohibition on Function Expansion

Participant Organizations shall not apply any analytic capabilities, artificial intelligence tools, or automated identification technologies, including facial recognition software or other external analytical tools, to personal information disclosed for the Common Program without the express prior approval of the Governance Partners and assessment under this PIA.

5.5 Disclosure of Personal Information

Personal information collected through the Common Program may only be disclosed where authorized under FIPPA and is necessary to support the purposes of the Common Program. All disclosures must remain directly connected to the purpose for which the personal information was collected. The permitted disclosure activities are set out in sections 5.5.1 to 5.5.6 below.

s.15

s.15 At all times, authorized City operators control what is displayed in the command room. Operational Partners present in the command room may observe only and do not retain independent access to video footage or personal information.

Event Alerts are brought to the attention of a CCTV Operator and may be broadcast to members with s. 15 access within the EOC. Where an incident requires a coordinated response, more detailed information may be displayed to the extent necessary to coordinate that response among relevant Operational Partners. Where more detailed information is relevant to only a limited number of Operational Partners, efforts will be made to review that information in the operational side rooms. Disclosure of personal information to Operational Partners in these circumstances is limited to what is reasonably necessary for the coordination of the operational response. Some disclosure of personal information to Operational Partners within the EOC is necessary to support the operational coordination of the Common Program. As set out in section 4.4 of this PIA, the City and VPD are satisfied that the EOC cannot reasonably function as an operational hub without this disclosure, and that such disclosure is proportionate to the public safety purposes of the Common Program. and cannot reasonably be avoided in the context of a multi-agency emergency operations environment.

The VPD will also operate its own Command Centre to coordinate its responses. s.15 s.15 The VPD operates this centre with its own operations personnel, who will have the same authority over the screen as the City's operators.

Authorized disclosures may occur between Participant Organizations for the purposes of:

- coordinating operational activities within the program zones;
- supporting situational awareness and incident response;
- assisting operational personnel responsible for safety, security, or program management;
- documenting and responding to incidents occurring within program zones; and
- supporting lawful investigations or compliance activities conducted by authorized law enforcement agencies.

Disclosure may include:

- live visual monitoring information communicated verbally or through secure operational channels;
- recorded video footage;
- still images extracted from recorded footage;
- contextual information associated with the video record, such as time, location, and incident description; and
- analytics outputs derived from camera systems where such outputs are necessary to support the operational purposes of the Program.

All disclosures will remain directly connected to the purposes for which the personal information was collected.

5.5.1 Real-Time Operational Disclosure ("Eyes-in-the-Sky" Communication)

Participant Organizations authorized to monitor the Camera System, may disclose relevant situational information observed through the Camera System to their own authorized personnel, and where necessary for operational coordination or incident response, to authorized personnel of other Participant Organizations

Information derived from the Camera System may be communicated between authorized personnel within Participant Organizations where such communication is reasonably necessary to support operational coordination, incident response, or situational awareness.

Such communication may include:

- real-time verbal updates;
- operational briefings;
- radio communications;
- secure operational messaging; or
- other communication channels approved by a Governance Partner.

Participant Organizations will ensure only personnel with a legitimate operational need have access to information derived from camera systems. Such disclosure supports real time situational awareness across the designated program zones, commonly referred to as an “eyes-in-the-sky” situational awareness function. Only information necessary to support operational coordination or incident response may be communicated.

5.5.2 Disclosure of Analytics Outputs

The Camera System generates analytic outputs, including Event Alerts or metadata derived from video analysis. Searchable metadata and activity summaries are accessible only to authorized City and VPD operators with the VMS and s.15 environment. Event Alerts are made available to authorized Governance Partner operators and users who have been provisioned to receive them.

Analytics outputs may be disclosed among Participant Organizations on an as-needed basis where necessary to support situational awareness, safety, and security operations of the Common Program.

However, the following principles apply:

- Analytics outputs are not disclosed externally as standalone datasets.
- Any external disclosure involving analytics outputs must be based on the underlying video footage and applicable legal authority.
- Analytics outputs are not used or disclosed in a manner that enables identification of individuals beyond the operational purposes of the Common Program.
- Analytics outputs are not relied upon in isolation from the underlying video footage.

Analytics outputs, including Event Alerts, may contain personal information and are subject to the same disclosure authorities and limitations as the underlying video footage.

5.5.4 Aggregated and Statistical Reporting Disclosures

Participant Organizations may disclose aggregated statistical information or heatmap images derived from Camera System data for purposes such as program reporting, evaluation, or public transparency.

Such disclosures may occur only where:

- personal information has been aggregated and/or de-identified; and
- the risk of re-identification has been assessed and reasonably mitigated.

Aggregated reporting may include information such as:

- incident counts;
- attendance counts;
- aggregated population flow heatmaps;
- operational activity summaries;
- general patterns or trends observed within Comon Program zones.

Aggregated reports will not include images, video, or information that could reasonably identify an individual.

5.5.5 Limitations on Disclosure

Participant Organizations will ensure that disclosure of personal information derived from the Camera System is limited to what is reasonably necessary to support the purposes of the Common Program. Personal information will not be disclosed where such disclosure is unrelated to Common Program purposes or where lawful authority for disclosure does not exist under FIPPA, applicable federal legislation, or the contractual arrangements established under the Common Program.

Further, Governance Partners will ensure that access to camera footage and related information is restricted to personnel with a legitimate operational need within the scope of the Common Program.

5.5.6 Prohibited Disclosures

The following disclosures are expressly prohibited unless authorized by law and approved by a Governance Partner:

- disclosure of camera footage or images for commercial purpose;
- disclosure of footage or images to external parties for research, marketing, or technology development purposes;
- subsequent disclosure of camera footage, images, or derived data to any partner organization or third party for the purpose of facial recognition technology (FRT);
- disclosure of analytics metadata or alerts as independent datasets for external analysis, except as required for technical support analysis;
- disclosure of camera footage or images to media or the general public unless authorized under applicable legislation;
- disclosure of personal information for purposes unrelated to the Common Program;
- disclosure of personal information collected through the camera systems for technology testing, artificial intelligence training, or other secondary purposes unrelated to the Common Program.

5.5.7 Disclosures outside of the CPA

There will be no real-time disclosure of video feeds to parties who are not signatories to the CPA. The City or VPD may, however, disclose video recordings or information derived from

video feeds to non-parties where authorized under FIPPA. Such disclosure may include incident reports or situational updates disclosed in accordance with FIPPA, or video recordings disclosed to a law enforcement partner for the purposes of specific investigation or prosecution under applicable law enforcement disclosure authorities.

PART 6 – ADVANCED TECHNOLOGY AND AI CAPABILITIES

6.1 Overview of Camera System Technology Stack

This section reviews the core underlying platform technologies and the analytics capabilities used to assist this program.

6.1.1 Core Video Management Platform s.15

The Common Program relies on an enterprise-grade Video Management System (VMS) to manage the collection, storage, access, and review of video footage captured by network-connected cameras deployed across program zones. The VMS provides centralized administration of camera devices, user roles, access controls, recording rules, audit logs, and system health monitoring.

The VMS functions as the system of record for all video collected within the Camera System and is used to provide authorized users with access to live and recorded video via VMS-controlled interfaces at authorized viewing stations only. All downstream analytics operate on video streams or recordings managed by the VMS and do not bypass VMS-level security, access controls, or retention rules.

6.1.2 Video Analytics Platform s.15

The Common Program incorporates an advanced video analytics platform that integrates with the VMS to enable accelerated forensic review, real-time alerting, and aggregated statistical analysis of video data. The analytics platform does not replace the VMS but consumes authorized video streams or recordings for analytic processing in accordance with the use limitations and prohibitions set out in section 5.4.6, 5.4.8, and Part 6 of this PIA.

The analytics platform processes video to generate structured metadata describing detected objects, movements, and events. This metadata is used to support search, filtering, alerting, and reporting functions accessible only to authorized City and VPD operators with the VMS and s.15 environment. Event alerts generated by s.15 are pushed from VMS to the Common Operating Platform, where they are made available only to Governance Partners users who have been provisioned to receive Event Alerts.

Event Alerts are generated by s.15 and may be made available through the Common Operating Platform to a limited number of Governance Partner users who have been specifically authorized to receive them based on role and operational need.

Key characteristics relevant to privacy and compliance include:

- s.15

- Centralized configuration and governance of Camera Systems across multiple sites and program zones. Role-based access control (RBAC) that restricts access to live and recorded video based on operational need. How this access is configured is discussed in Section 7.4 below.
- Integration with s.15 s.15 s.15 This is used to support the analytics platform, described below.

6.1.3 Common Operating Platform

The Common Operating Platform is a situational awareness dashboard used within the Common Program's technical environment. It sits downstream of the Camera System and is used within the City's Emergency Operations Centre (EOC) as part of the Command, Control, Coordination, and Communication (C4) environment to display selected operational information.

The Common Operating Platform does not collect, store, or analyze video footage or personal information and does not perform analytics or decision-making functions. In relation to the Camera System, the Common Operating Platform renders for display Event Alerts that are generated through the Video Management System (VMS and associated analytics). Event Alerts are derived information and, in some circumstances, may include personal information, consistent with the authorized purposes of the Common Program.

The Common Operating Platform does not provide access to live or recorded video footage, does not enable interaction with analytics, and does not function as a system of record. Displaying information through the Common Operating Platform does not change how personal information is collected, used, disclosed, retained, or governed under the Camera System. All video footage, analytics processing, access controls, and disclosure authorities remain governed exclusively through the VMS and the Common Program framework described in this PIA.

6.2 AI and Automated Analytics

This section describes the AI-enabled video analytics capabilities enabled through the Video Management System (VMS) under the Common Program. Analytics deployed through the VMS are configured and used as decision-support tools to assist authorized personnel in identifying situations requiring review. While prospectively capable, the system is not configured to allow the City or the VPD to use any facial recognition through s.15 the s.15 Platform (VMS), or any other technologies within this Common Program.

6.2.1 Nature of AI-Enabled Functions

The s.15 analytics platform applies pre-trained machine-learning and computer-vision models to video footage to identify and classify objects and activities captured by cameras. The following analytics capabilities are deployed under the Common Program and are described in detail in Annex C (AI Model and Analytics Register):

- Extraction of descriptive attributes (e.g., direction of travel, speed, dwell time, size, color). This is done manually when an alert, such as a vehicle in a pedestrian area or line crossing has been triggered, not through the analytics themselves.

- Temporal indexing of activity to enable rapid review across extended time periods
- Generation of event-based alerts when predefined conditions are met, such as line crossing or vehicles in a pedestrian area
- Aggregation of counts and movement patterns for statistical and trend analysis

The s.15 analytics platform includes functionality that can significantly reduce the time required to review large volumes of video footage by presenting condensed visual summaries and filtered search results. Analytics outputs are indicative only and are used to draw attention of authorized operators to footage or situations requiring review. Automated analytics outputs are generated continuously but require human review and validation before any operational action is taken, as described in sections 6.2.2 and 6.2.3. Access to analytics outputs is subject to the access controls and use limitations set out in section 5.4.6 and 7.4.

6.2.2 Decision-Support vs. Decision-Making

Analytics outputs are used solely to assist authorized operators in identifying situations requiring attention and locating relevant footage. No operational or enforcement decisions are about individuals on the basis on analytic outputs alone. Human operators remain responsible for all interpretation, decision-making, and any subsequent response, as described in section 6.2.3

The Camera System does not make automated decisions about individuals or events.

More specifically:

- Analytics outputs are used to assist Camera System Operators in locating relevant footage or identifying situations requiring attention.
- Alerts generated by the system require human review and validation before any operational action is taken.
- No automated enforcement, sanctions, or determinations are made solely on the basis of analytics outputs.
- Human operators, particularly in the City EOC and VPD Ops Centre, and local zone security offices remain responsible for interpreting analytics outputs, making operational decisions, and directing any subsequent response.

6.2.3 Human-in-the-Loop Controls

The Common Program requires that:

- Video analytics alerts are reviewed prior to any operational action;
- Video footage is manually verified against original footage before being relied upon for investigative or operational purposes; and
- Access to video analytics interfaces is limited to authorized users in accordance with the role-based access controls set out in section 7.4.

As noted above, video analytics alerts are used solely to draw, the attention of authorized operators, to a potential issue requiring review. Operators stationed at the City EOC, VPD DOC, or local zone security offices review the relevant footage and, where necessary, relay information to authorized personnel on the ground to investigate or manage a situation.

6.3 Model Governance

6.3.1 s.15 Model Training and Updating

The s.15 analytics platform uses pre-trained computer vision models provided by the vendor. The Common Program does not conduct custom model training using program-specific video data. Any future proposal to introduce custom model training using program specific data would require prior approval through the Change-Management Process and an updated PIA review as set out in Section 11.1.

Vendor updates will not apply to this program as the Camera System is only operating for a short period of time. The Governance Partners do not anticipate any updates that could substantively alter their abilities or the assessment of this program within that short period of time.

6.3.2 Bias and Accuracy Considerations

The s.15 analytics platform generates probabilistic outputs that may be affected by environmental conditions such as lighting, camera angle, crowd density, and occlusion. The Governance Partners recognize the potential for false positives, false negatives, and uneven performance across contexts. This is a predominant reason for ensuring that analytics are not relied upon in isolation and that only humans are making decisions based on an independent review of the underlying video footage prior to any operational action.

Mitigation measures include:

- Restricting reliance on analytics outputs without human confirmation;
- Using analytics primarily for triage, search, and situational awareness rather than determinations about individuals or situations; and
- Pre-event testing of analytics performance and alert thresholds.

6.3.3 Validation and Testing

The City conducted a full-scale exercise on April 16 ,2026 and ongoing testing and validation will continue up until FWC26. This included operational testing to ensure:

- Analytics configurations are tested in controlled environments
- Alert thresholds and use cases are validated against operational needs
- Use cases that materially increase privacy risk require documented approval

As a result of the exercise the Governance Partners have made minor operational adjustments to camera placement, system configuration, and developed specific operator training in advance of FWC26.

6.4 Risks of Inference and Re-Identification

The video analytics derived data and metadata are generated in support of the safety and security objectives of the Common Program. While the analytics functionality does not identify

named individuals, the creation and use of derived information introduce a risk that individuals could be indirectly identified or inferred through patterns, correlations, or repeated observations.

This risk may arise where analytics capture individuals repeatedly within predictable locations or timeframes or analyze movement patterns or dwell times over extended periods, or where analytics outputs are combined with other datasets. Certain capabilities, such as temporal indexing and rule-based alerting, may increase the sensitivity of the information even in the absence of direct identifiers.

To mitigate the risk of inference or re-identification, analytics are configured and governed in accordance with the principles of necessity, proportionality, and purpose limitation. Analytics are limited to clearly defined and documented purposes that are directly related to the Common Program's mandate, as described in this PIA. Analytics features that are not required to meet operational objectives are disabled or restricted.

The Common Program mitigation efforts include addressing the risks of inference and re-identification through:

- Limiting analytics to authorized purposes explicitly documented in this PIA and the AI and Analytics Register at Annex C;
- Disabling or restricting analytics features not required for program objectives;
- Applying strict access controls and audit logging to analytics outputs;
- Ensuring that derived metadata is treated with the same level of protection as underlying video footage; and
- Prohibiting secondary use of analytics outputs for unrelated purposes.

Derived data and metadata are protected at a level equal to the underlying video footage and subject to the same use, disclosure, and safeguarding requirements. Secondary use of analytics outputs for unrelated purposes is prohibited.

Residual risk remains that analytics outputs could, in limited circumstances, support inference about individuals when viewed in combination with other information. However, the application of technical controls, administrative safeguards, and governance restrictions significantly reduces the likelihood and impact of reidentification and ensures that analytics related privacy risks remain proportionate to the Common Program's objectives.

A simplified table-version of this information is found in the Risk Register, located in Annex D.

6.4.1 Risks associated with the Common Operating Program

The Common Operating Program functions solely as a situational awareness display and may present Event Alerts derived from the Camera System's video analytics to authorized users within the controlled EOC environment. While Common Operating Platform does not enable access to underlying video footage or analytics interfaces, the visual display of alerts introduces a limited risk that repeated exposure to alerts over time could contribute to inference about individuals, locations, or activity patterns.

This risk is mitigated through the same technical, administrative, and governance controls that apply to analytics outputs generally, including limiting alert content to what is necessary for situational awareness, restricting access to authorized users, prohibiting secondary use of

alerts, and ensuring that alerts are reviewed and contextualized by trained human operators. Display of alerts through the Common Operating Platform does not increase the sensitivity of the underlying information nor alter the collection, use, disclosure, retention, or governance framework described in this PIA.

PART 7 – SECURITY AND SAFEGUARDS

7.1 Technical Safeguards

The Common Program incorporates a layered set of technical safeguards designed to protect personal information from unauthorized access, collection, use, disclosure, alteration, or destruction. These safeguards are implemented through a combination of infrastructure controls, network security measures, system configuration, and access management processes.

7.1.1 Data Storage and Hosting

All video and associated with the Camera System data generated through the Common Program are stored on infrastructure located within the data centre located at s. 15 in Vancouver, Canada. It is a City managed and controlled technical environment. Data is retained on s. 15 operated by the City and/or authorized technical partners, rather than being stored in external commercial cloud environments.

The primary system infrastructure supporting the Common Program is hosted within a secured s.15 data centre environment. The physical and logical hosting location is subject to the City's enterprise security standards, including controlled facility access, environmental protections, network segmentation, and continuous monitoring. Details on the physical security of the location is below in section 7.2.

7.1.2 Network Connectivity and Transmission

The Camera System transmits video data to the central system infrastructure using secure wireless connectivity.s.15 s.15 s.15 . More details on this network are below in section 7.1.3.

The network architecture incorporates secure communication channels designed to prevent interception, tampering, or unauthorized access to data in transit.

Technical safeguards for data transmission include:

- Encrypted transmission of video and system data;
- Secure network routing through authorized telecommunications providers;
- s.15
- Monitoring and logging of network connections

7.1.3 5G Network Architecture and Implementation:

The Common Program relies on telecommunications infrastructure that utilizes s.15 s.15 to support secure and reliable transmission of video data from camera locations to the central system infrastructure.

s.15

operational requirements. Within this architecture, the Common Program's network traffic operates within a defined virtual network environment with controlled performance, routing, and security parameters that are separate from other commercial network traffic operating on the same carrier infrastructure.

s.15

Video data transmitted from cameras to the VMS is protected through encrypted transmission protocols and secure network routing. s.15 s.15, while the Common Program maintains responsibility for the security of its systems, devices, and data once received within the Common Program environment.

To support secure network operations, the network architecture incorporates multiple technical safeguards designed to protect video data while in transit and reduce the risk of unauthorized access or interception.

Technical safeguards for the network architecture include:

- s.15
- Encrypted transmission of video and system data across the telecommunications network s.15
- Secure routing of network traffic through authorized telecommunications providers;
- Monitoring and logging of network connectivity and system communications; and,
- Network segmentation between telecommunications infrastructure and municipal systems, as well as firewall protection through Fortinet.

The Program does not store video data within telecommunications provider infrastructure. All video data is received by the Program's systems and stored within secured s.15 infrastructure operated by the City or authorized technical partners, as described in Section 7.1.1.

7.1.4 Encryption and Data Protection

In addition, encryption and other data protection mechanisms are used to safeguard information both in transit and at rest within the system environment. This includes encryption protocols applied to video transmission and storage systems.

7.2 Physical Safeguards

Personal information processed through the Camera System is stored within the highly secured facility s.15 This facility is restricted to authorized personnel and protected through a combination of controlled entry points, monitored access, and security personnel. Physical access to the infrastructure supporting the Camera System is limited to individuals with operational responsibilities and is governed by formal access management procedures.

Operational viewing of Camera System data occurs only within designated secure environments. These environments include approved command or operational coordination locations established for the purposes of supporting authorized activities, within the Emergency Operations Centre itself, or within VPD's operations centre and local zone security offices established at Killarney Training Facility, UBC National Soccer Training Centre, and Fan Festival at the PNE. Access to these locations is restricted to authorized personnel and subject to on-site security controls, including controlled entry, credential verification, and supervision where appropriate.

Within these secured locations, the Camera System data may only be accessed using designated devices that have been specifically configured and assigned for this purpose. These devices are maintained within the secured operational environment and are not intended for general use. Access to system data is limited to personnel whose roles require such access in order to perform authorized operational duties, and controlled with role-based access, as described below in section 7.4.

No public-facing or general-purpose terminals are used to access the Camera System. The restricted physical environment, combined with role-based authorization controls, ensures that personal information is only accessible within controlled and monitored operational contexts.

7.3 Administrative Safeguards

The Governance Partners have implemented administrative safeguards are implemented to ensure that access to personal information within the Camera System is limited to authorized personnel and that such access occurs only for legitimate operational purposes. These safeguards include governance controls, defined roles and responsibilities, operational procedures, training requirements, and oversight mechanisms designed to support compliance with applicable privacy and information-security obligations.

7.3.1 Governance and Accountability

Governance Partners maintain clear governance structures that define responsibility for the operation of the Camera System and the protection of personal information processed within it. Designated Governance Partner leads and system administrators are responsible for ensuring that Camera System use complies with applicable legislation, internal policies, and approved operational procedures**.** Operational Partners are responsible for ensuring their personnel comply with the privacy, security, and operational requirements ser out in the CPA.

Access to Camera System data is limited to Governance Partner personnel or contractors whose roles require such access to perform authorized operational duties. Authorization to access the system is granted through established access-management processes and must be approved by designated supervisors or system administrators.

Access privileges are role-based and limited to the minimum level necessary to perform assigned responsibilities Access management processes governing the Camera System are described in Section 7.4.

7.3.2 Training and Awareness

The Governance Partners will provide training to authorized personnel regarding the privacy, confidentiality, and information-handling obligations associated with accessing the system. This privacy training complements operational and technical training provided by program operators and system administrators. The privacy training focuses on ensuring that personnel understand the legal authorities governing the collection, use, and disclosure of personal information, as well as the safeguards and restrictions applicable to the Common Program.

Depending on their role, training includes instruction on:

- Obligations under applicable privacy legislation;
- Responsible handling of personal information, including using video analytics for decision support only;
- Appropriate and authorized uses of the Camera System;
- Disclosure rules and how to share information appropriately;
- Retention and handling of footage;
- Security practices related to device handling and operational environments; and
- Procedures for reporting suspected privacy breaches or security incidents.

Privacy training is provided prior to Camera System access being granted and may be supplemented by periodic refresher training where operational procedures or privacy requirements change.

7.3.3 Monitoring, Logging, and Oversight

Access to the Camera System and Camera System activities are subject to logging and monitoring controls designed to support accountability and oversight. Camera System logs may record activities such as user authentication, system access, data queries, and export actions. These logs may be reviewed periodically to ensure that Camera System access and use remain consistent with authorized purposes and operational procedures.

Where appropriate, supervisory review processes may be implemented to ensure that access to personal information is justified and consistent with established policies and procedures. The logging and monitoring framework, including responsibility for log review, frequency of review, and follow up procedures, is described in section 7.4.7.

7.3.4 Incident and Breach Management

Participant Organizations and their personnel, including Governance Partner personnel, Operating Partner personnel, and contracted service providers, maintain incident response procedures for addressing potential privacy or security incidents involving personal information collected under the Common Program. Governance Partner personnel are required to promptly report suspected incidents, to their designated program lead. Operational Partner personnel and contracted service providers are required to promptly report suspected incidents directly to Governance Partners. Suspected incidents include lost devices, unauthorized access, or other potential compromises involving personal information.

Reported incidents are assessed and managed in accordance with established breach-management procedures, which may include containment measures, investigation, notification where required, and implementation of corrective actions to reduce the likelihood of recurrence.

The Governance Partners are responsible for coordinating incident response across all Participant Organizations. Incidents involving personal information collected under the Common Program must be reported to the Governance Partners within the timeframe specified in the CPA.

7.3.5 Confidentiality Obligations

Governance Partner personnel with authorized access to personal information collected under the Common Program are subject to confidentiality obligations as a condition of their employment. Operational Partner personnel are subject to confidentiality obligations as a condition of their organization's participation in the CPA. Contracted service providers are subject to confidentiality obligations under the contractual agreements with the City. These obligations require protection of personal information from unauthorized access, use, or disclosure and to access such information only when required for authorized operational purposes.

Failure to comply with these obligations may result in disciplinary action for Governance Partner personnel in accordance with applicable employment policies, or remedies under the CPA or applicable contractual arrangements for Operational Partner personnel and contracted service providers.

7.3.6 Contractual Security and Compliance Obligations

Participation in the Common Program requires Participant Organizations and their authorized personnel to comply with the privacy, security, and operational requirements set out in the applicable agreements.

These contractual obligations include requirements to:

- Access personal information only for authorized Common Program purposes;
- Limit access to personnel with operational need-to-know;
- Implement appropriate administrative, physical, and technical safeguards;
- Protect information from unauthorized access, use, or disclosure;
- Report privacy or security incidents in accordance with established procedures; and
- Comply with applicable retention, audit, and oversight provisions.

The agreements also provides mechanisms for oversight and accountability, including the ability to review compliance with the agreement and to address instances of non-compliance where necessary.

7.4 Access Controls and Auditability

7.4.1 System Access

Access to personal information within the Camera System is governed through a role-based access control (RBAC) framework designed to ensure that individuals only access information necessary to perform authorized program functions. Access permissions are assigned based on defined operational roles and the principle of least privilege, meaning users are granted the minimum level of access required to carry out their duties.

The Camera System includes seven distinct user roles, each with different permissions relating to the viewing, use, and export of information. These roles include operational users, administrative users, and training or testing accounts.

A detailed description of the permissions associated with each role, including the ability to view live data, access non-live or archived information, and export data, is provided in the table below:

CCTV Account Matrix

Account	Camera View	View – Live	View – Historical Video & Investigative Analytics	Export Data
s.15				

Access permissions are configured so that users may only access information necessary for their operational responsibilities within the program.

Access to the Camera System is granted only after:

- Confirmation of an operational requirement for access;
- Approval by the applicable Governance Partner and provisioning by the designated System Administrator responsible for user access approvals (e.g., system administrator, program manager, or other delegated authority); and
- Completion of applicable privacy or security training, as identified in section 7.3 above.

Access is authenticated through the Camera System's identity management functions, configured by the Governance Partners.

User access is removed or modified when personnel change roles, no longer require access to perform their duties, or cease employment with the Participant Organization.

7.4.2 Secure Devices and Encryption

Access to Camera System data is restricted to a limited number of designated laptop devices that are configured specifically for secure Camera System access. These devices are provisioned and managed in accordance with the City's information security standards.

Each authorized device incorporates multiple technical safeguards, including:

These safeguards ensure that data stored locally on authorized devices is protected against unauthorized access. If a device is lost or stolen, encryption safeguards prevent unauthorized parties from accessing the information stored on the device. This control significantly reduces the risk that personal information could be accessed or disclosed in the event of device loss, theft, or unauthorized physical access.

7.4.3 Live Operational Data

As described above, Operational Partners, in addition to Governance Partners, will have access to live data, also referred to as collection through observation. Access to live data is restricted to Participant Organization personnel whose duties require monitoring or responding to system alerts, operational events, or program activities.

Further, as noted in the table in section 7.4.1, local security offices only have the ability to view live camera feeds for their specific zone. They do not receive alerts through the Common Operating Program. Should an alert affect their zone and require action, the EOC or relevant VPD command centre will coordinate the response.

The following safeguards apply to live data access:

- Participant Organization personnel may view information as displayed on the screen or in the event of an incident, may work with their Governance Partner to request that the operations room operator to adjust the camera view.
- Only designated Governance Participant personnel may authorize the retention of data. All other Participant Organizations must request the retention of footage and provide a rationale for data export, in accordance with the provisions of the Common Program Agreement.
- Access to live Camera System environments is limited to local one security offices, the Emergency Operations Centre, and the VPD Command Centre.

These controls are intended to ensure that live information is accessed only for authorized Common Program purposes and that the potential for unauthorized disclosure is minimized.

7.4.4 Stored or Retained Data

Access to non-live Camera System data, being footage and associated records retained in accordance with Section 9.1, is limited to authorized Governance Partner operators and contracted service providers in accordance with the RBAC set out in section 7.4.1. Requests to access retained footage must be documented and approved by a Governance Partner for a specific operational purpose consistent with the authorized uses set out in section 5.4. All access to non-live Camera System data is subject to audit logging as described in section 7.4.7.

Non-live data refers to information retained in the system after operational use, including stored, archived, or indexed records. Access to non-live data is limited to users who require access for authorized program functions such as:

- operational review;
- investigation or incident response;
- compliance monitoring;
- authorized program evaluation or analysis; or
- system testing or training activities.

Training or testing environments use non-production datasets, de-identified information, or other privacy-protective methods wherever feasible to reduce exposure to personal information.

Where COV and VPD authorized operators access archived records, access must be connected to a legitimate operational purpose and must be consistent with the program's authority to use the information.

7.4.5 Data Export Controls

Export functionality is restricted to s.15 accounts as set out in the RBAC table in section 7.4.1. As exporting data increases the risk of unauthorized disclosure, export capabilities are only provisioned for these authorized roles and permit extraction of video footage and alerts from the system, when required for approved operational purposes. Audit logs for extraction are triggered and the following purposes for extraction are approved:

- an active investigation or operational incident;
- a request made under lawful authority; or
- another Common Program activity authorized under applicable legislation or operational policy. In these cases the authorizing legislation or operational policy is documented.

When exporting data, the following safeguards apply:

- authorized users must limit exported information to the minimum amount necessary to fulfill the authorized purpose;
- exports must be associated with a documented operational justification such as a file number, incident number, or authorized request identifier;
- exported Camera System data must be stored and handled in accordance with the information security and records management policies of the receiving organization.

Export activity is recorded in Camera System audit logs and subject to periodic review to ensure exports are limited to the minimum information necessary and are consistent with authorized Common Program use.

7.4.6 Log Retention

Audit logs are retained for the period specified in the applicable security or records retention schedule of the applicable Governance Partner. Retention periods are designed to ensure logs remain available long enough to support:

- investigation of privacy incidents;
- detection of unauthorized access;
- internal or external compliance reviews; and
- operational security monitoring.

Following the applicable retention period, logs are securely disposed of in accordance with the approved records management and disposition schedules of the applicable Governance Partner.

Further information about retention periods is found in Part 9.1 of this PIA.

7.4.7 Monitoring and Review

Camera System activity logs are subject to periodic monitoring and review to identify unauthorized access, anomalous behavior, or potential misuse of personal information collected under the Common Program.

Monitoring activities may include:

- automated monitoring or alerting mechanisms within the Camera System;
- periodic compliance reviews conducted by authorized City system administrators or designated Governance Partner oversight personnel; and
- targeted reviews triggered by complaints, suspected misuse, or privacy incidents.

Where inappropriate access or use of personal information is identified, the matter may be investigated in accordance with the privacy breach management procedures outlined in the Common Program Agreement.

User access permissions are reviewed in the event of attempted unauthorized access. Otherwise, this Common Program is short-lived and does not warrant an extensive periodic access review program.

7.4.8 Privacy Safeguards

The safeguards described in this Section 7 support the obligation of public bodies to protect personal information using reasonable security arrangements against risks such as unauthorized access, collection, use, disclosure, or disposal.

Access controls, export restrictions, and system logging collectively ensure that personal information collected under the Common Program is subject to controlled access, documented use, and auditable oversight consistent with FIPPA and the governance obligations of this PIA.

7.5 Approval and Oversight

The Common Program operates under a defined governance and oversight structure intended to ensure that the deployment and use of camera technologies occur in a manner that is lawful, proportionate, and consistent with applicable privacy and security obligations.

7.5.1 Decision Authority

Authority for the approval, deployment, and operational use of the Common Program rests with the Governance Partners in accordance with the Common Program Agreement.

The Governance Partners retain responsibility for:

- approving the deployment and operational parameters of the Common Program;
- determining authorized uses of the Camera System and associated technologies;
- establishing operational policies and procedures governing access and use;
- approving the participation of Operational Partners in accordance with the CPA; and
- ensuring compliance with applicable legal and regulatory requirements.

Operational decision-making related to day-to-day Camera System use may be delegated to authorized Governance Partner personnel responsible for program administration, monitoring, and coordination activities. Such operational decisions must remain consistent with the Common Program's approved governance framework and documented operational policies.

7.5.2 Ongoing Monitoring and Oversight

The Governance Partners will conduct ongoing oversight of the Program to ensure continued compliance with legal, privacy, and operational requirements.

Oversight activities include:

- monitoring Camera System access and usage logs;
- reviewing Camera System activity to ensure compliance with authorized purposes;
- assessing adherence to established operational procedures and governance agreements;
- evaluating Camera System performance and operational effectiveness; and
- reviewing privacy and security controls associated with the Common Program.

Periodic internal reviews may be conducted to confirm that the Common Program continues to operate in accordance with its approved purposes and governance framework.

Where appropriate, the City, as the primary technical operator of the Camera System, may also review system configurations, retention practices, and access permissions to ensure they remain aligned with applicable privacy and security requirements throughout the operational period.

Any identified issues relating to privacy, security, or Common Program compliance will be addressed through agreement between the Governance Partners and may include corrective action, policy adjustments, or updates to operational procedures as required.

Material changes to the Common Program that may affect the collection, use, disclosure, or protection of personal information may be subject to further privacy review or assessment in accordance with applicable policies and procedures.

7.6 Security and Safeguards Risk Assessment

While the technical, administrative, and governance safeguards described above significantly reduce privacy risks associated with the Common Program, certain residual risks remain inherent in the Camera Systems involving the collection and management of visual recorded data.

This section identifies privacy risks that may arise from the Camera System infrastructure, network architecture, and operational controls described in this Section 7, as well as the mitigation strategies implemented to address those risks. A simplified table-version of this information is found in the Risk Register, located in Annex D.

7.6.1 Physical Security Risks

The Common Program includes operational monitoring stations and centralized Camera System infrastructure that contain or provide access to personal information collected under the Common Program. As with any physical environment containing systems that process personal information, there is a potential risk that unauthorized individuals could gain physical access to Camera System equipment or viewing environments. s.13(1) s.13(1) s.13(1)

Operational viewing stations are staffed by authorized security personnel responsible for monitoring system activity. These facilities operate within secured environments that include controlled entry points and restricted access procedures.

Similarly, the data centre environment hosting the system infrastructure is located within a secured facility that uses s.15 s.15 s.15. These physical security measures reduce the likelihood of unauthorized access to systems or monitoring environments.

s.13(1)

7.6.2 Administrative Safeguards and Personnel Access

As system monitoring and operational coordination involve human interaction with surveillance systems, there is an inherent risk that authorized personnel could access or use system data outside the scope of their assigned responsibilities. The Common Program mitigates this risk through administrative safeguards governing system access and operational procedures.

Access to the system is limited to personnel with authorized operational roles. Users are assigned system permissions based on their responsibilities, and operational procedures govern when and how system data may be accessed or retrieved. Personnel who operate or access the system are subject to the City's applicable policies, procedures and oversight mechanisms relating to information handling and privacy protection. s.13(1)

s.13(1)

7.6.3 Access Controls and Role-Based Permissions

The system incorporates a robust role-based access control (RBAC) framework designed to restrict system access based on user roles and operational responsibilities. Under this model, users are granted only the level of access necessary to perform their duties. Administrative privileges are restricted to authorized system administrators, while operational users may access system functionality appropriate to their roles.

This approach reduces the risk of unauthorized system access or misuse of system capabilities.

s.13(1)

7.6.4 Auditability and Monitoring

Systems that enable access to video footage must maintain appropriate logging and audit capabilities to ensure accountability and detect potential misuse. The Common Program's system environment maintains logs of user activity related to system access and the retrieval of video footage. These logs enable administrators to review when footage has been accessed, by whom, and for what operational purpose.

Audit logging supports oversight activities and enables investigation of potential unauthorized access or misuse of system data. s.13(1)

s.13(1)

s.13(1)

7.6.5 Unauthorized System Access

Systems that contain visual camera footage data may present risks if unauthorized individuals gain access to the system or if authorized users access data outside of their operational responsibilities. The Common Program mitigates this risk through a combination of role-based access controls, authentication requirements, and system logging. Access to the system is restricted to authorized personnel with operational responsibilities related to monitoring, coordination, or investigation support.

System activity, including user access and data retrieval actions, may be logged and monitored to detect potential misuse or unauthorized access. s.13(1)
s.13(1)

7.6.6 Data Storage and Infrastructure Risks

As with any information system, there is a risk that unauthorized access or compromise of the underlying infrastructure could result in unauthorized access to stored data. The Common Program mitigates this risk by storing system data within controlled infrastructure environments subject to municipal security standards, including restricted physical access, system hardening, and network security controls.

Data storage systems are maintained within the City's controlled s. 15
rather than external commercial cloud platforms, reducing exposure to third-party data processing risks. s.13(1)

7.6.7 System Configuration and Technology Risks

Complex systems that integrate cameras, network infrastructure, analytics tools, and monitoring platforms may present risks if system configurations are misconfigured or if new features are introduced without appropriate governance oversight. To mitigate this risk, system configuration and changes to system functionality are subject to governance oversight and operational procedures. Material changes to system capabilities that could affect the collection, use, or disclosure of personal information may require additional privacy review.

In addition, contractual and technical controls are used to limit the deployment of features that could introduce additional privacy risks, including the use of technologies such as facial recognition. s.13(1)
s.13(1)

7.6.8 Operational Oversight

The combination of physical security measures, role-based access controls, audit logging, and governance oversight provides multiple layers of protection designed to safeguard personal information within the VMS. While no system can eliminate all risk, the safeguards implemented significantly reduce the likelihood that personal information processed through the VMS could be accessed, used, or disclosed inappropriately.

The City will continue to monitor the effectiveness of these safeguards and adjust operational practices or technical controls as necessary to address emerging risks.

7.6.9 Partner Access and Information Sharing

As the Program involves the coordination with Participant Organizations, including public safety and operational partners, there is a risk that information could be accessed or shared outside the scope of the Program's authorized purposes. This risk is mitigated through governance agreements, operational protocols, and access controls that restrict system access and information disclosure to authorized circumstances and legal authorities.

Analytics outputs and alerts generated by the system are not disclosed externally as standalone datasets. Any disclosure of information derived from the system must rely on underlying video footage and applicable legal authority.

s.13(1)

PART 8 – ACCESS, TRANSPARENCY, AND INDIVIDUAL RIGHTS

8.1 Collection Notification

A layered collection notification approach will be used across the Common Program. At the program level, a standardized notice published on the City's FWC26 website will communicate the overall purpose of the initiative, the types of personal information collected, and key contact information.

Clear, prominent signage will be placed at entry points to each zone, providing advance notice before individuals enter monitored areas. These signs will identify the applicable zone and indicate the nature of monitoring activities. This approach is supplemented by zone-specific adaptations to reflect differing operational contexts. In Hotel and Entertainment zones, additional localized signage will be deployed to reflect site-specific operations.

Sample signage is provided in Annex E, with standardized wording set out in Section 5.3.2 above.

8.2 Accuracy Standards

8.2.1 Accuracy Assurance Mechanisms

The Common Program recognizes that video footage and associated analytics outputs may inform operational decision-making by authorized personnel. Accordingly, the Common Program implements technical, operational, and governance measures to support the accuracy and reliability of information derived from the Camera System.

Video data is collected through fixed cameras and managed through the Common Program's VMS. Authorized users may review live or recorded video streams and may utilize analytics outputs generated by the analytics tool to assist with identifying relevant video segments.

To support accuracy and reduce the risk of misinterpretation:

- **Human Verification Requirement**
  Automated analytics outputs (including alerts, object classifications, or event indicators) are treated as decision-support tools only. Authorized Governance Partner operators must review the underlying video footage before relying on analytics outputs for operational coordination or investigative purposes, as described in section 6.2.3.

- **Operator Training and Procedures**
  Governance Partner personnel and contracted service providers authorized to access the Camera System receive training on:
  - the capabilities and limitations of the Camera System's video analytics tools,
  - appropriate interpretation of visual information,
  - procedures for confirming events through manual review of footage.
  - their obligations for the Common Program and FIPPA

- **Contextual Interpretation Controls**
  Authorized operators are instructed to interpret Camera System video footage within its operational context and to avoid drawing conclusions based solely on automated classifications or isolated frames.

- **Audit and Oversight**
  Access to video footage and the retrieval of clips are logged within the VMS in accordance with the audit logging framework set out in Section 7.4.6. These audit records enable monitoring of Camera System use and support review if questions arise regarding the interpretation or use of information derived from the system.

- **Technology Configuration and Maintenance**
  Camera System and analytics systems are configured and maintained by City technical administrators in accordance with vendor specifications and operational requirements to support consistent image capture and analytics performance.

Together, these mechanisms ensure that the Camera System outputs are used appropriately and that any operational decisions are based on verified visual information rather than automated analytics alone.

8.2.2 Data Quality Controls

The Governance Partners implement a range of measures to maintain the integrity and quality of Camera System video data and associated analytics outputs.

- **Camera Configuration and Maintenance**
  Cameras are installed and maintained by City system administrators to support appropriate image clarity, positioning, and field of view for operational purposes. Maintenance activities may include adjustment of camera positioning, firmware updates, and verification of system connectivity to ensure reliable capture of video data.

- **System Integration Controls**
  Video footage captured by cameras is stored within the EOC's on-prem data centre and managed within the VMS, as described in section 7.1.1. Analytics processing performed by s.15 relies on the underlying video footage maintained within the VMS, ensuring that any analytics output can be validated against the original source footage.

- **Validation Through Source Footage**
  Analytics metadata, alerts, or search results generated by the Camera System are not treated as authoritative records in isolation. Authorized operators must review the corresponding source video footage within the VMS to confirm the accuracy and relevance of analytics results before any operational reliance.

- **Limitations of Automated Classification**
  The Governance Partners recognize that automated s.15 analytics may produce false positives, incomplete detections, or classification errors due to environmental conditions such as lighting, weather, crowd density, or camera angle. Common Program policies therefore prohibit reliance on analytics outputs without human review.

- **Prohibition on Certain Uses**
  To reduce risks associated with inaccurate or biased identification, the Common Program does not utilize facial recognition technology capabilities within the Camera System.

- **Periodic Review of System Performance**
  City system administrators periodically review Camera System performance and may adjust configurations or workflows where necessary to maintain effective system operation and data quality.

8.2.3 Accuracy Risk Mitigation

Given the operational nature of the Camera System, it is not possible to guarantee that all captured images or analytics outputs will be complete or error-free. The Common Program mitigates this risk through:

- reliance on human verification of footage by authorized Governance Partner operators,
- training and operational procedures for Camera system users,
- technical maintenance and monitoring of Camera System performance, and
- governance controls restricting the use of analytics outputs without validation.

These measures support the reasonable accuracy of personal information used within the Common Program while recognizing the inherent limitations of video-based technologies.

8.3 Correction and Annotation

The Governance Partners recognize that individuals have the right to request correction of personal information held by a public body where the information is inaccurate or incomplete. Given the nature of the Camera System, correction and annotation processes focus primarily on associated metadata, contextual descriptions, and administrative records, rather than alteration of original video footage.

The Governance Partners have established procedures to ensure that correction requests can be addressed appropriately while maintaining the integrity of original records and ensuring consistent handling among Participant Organizations.

8.3.1 Integrity of Original Video Records

Video footage captured within the VMS constitutes an unaltered record of events as recorded by the Camera System at a specific point in time. As such, original video files are maintained in their original form and are not modified in response to correction requests.

Maintaining the integrity of original footage is necessary for several reasons:

- **Authenticity and Evidentiary Integrity**
  Video recordings may be relied upon for operational decision-making, investigations, or legal proceedings. Altering the original footage could compromise the authenticity of the record and undermine its evidentiary value.

- **Records Management Requirements**
  Public bodies are required to maintain records in a manner that preserves their integrity and reliability as official records. Editing or altering video files after capture could compromise the accuracy and reliability of the record as originally created.

- **Technical System Integrity**
  The VMS is designed to preserve captured footage as a secure, time-stamped record. Modifying video files would interfere with Camera System audit trails, retention controls, and chain-of-custody mechanisms that support accountability and oversight.

For these reasons, original video footage is not altered or edited to correct perceived inaccuracies.

8.3.2 Process for Requests to Correct or Annotate

Individuals who believe that personal information about them contained in VMS records is inaccurate or incomplete may submit a request for correction in accordance with applicable access and privacy legislation.

Correction requests may relate to information such as:

- descriptive metadata associated with video footage,
- incident summaries or operational notes created by authorized personnel,
- administrative records documenting the retrieval or use of video footage, or
- other records generated through the use of s.15 analytics.

Requests for correction will be submitted to the designated access and privacy contact of the applicable Governance or Operational Partner. Upon receipt of a request:

- The Governance or Operational Partner will review the record to determine whether the information is inaccurate or incomplete.
- Operational Partners will refer any request related to Camera System video footage or records to their paired Governance Partner from section 1.3.1 or 1.3.2.
- Where the request relates to Camera System records, the Governance Partner will verify the information against the underlying source footage and associated VMS system logs.
- If the request is determined to be justified, the responsible organization will correct the relevant record or metadata where technically feasible.

As original video footage represents a record of events as captured by the system, the VMS does not alter or edit original video files. Where a correction cannot be made to the original record, the Governance or Operational Partner will instead add an annotation noting the correction request and the individual's position regarding the accuracy of the information.

In some cases, individuals may request correction of records that describe, summarize, or reference video footage captured by the VMS, even where the video recording itself is not part of the record being corrected. These records may include incident summaries, operational notes, reports prepared by authorized personnel, or metadata generated through system searches or analytics tools. Such records are subject to the standard correction provisions applicable to personal information maintained by Participant Organizations.

Where a correction request relates to descriptive or interpretive information about video footage, the responsible Governance Partner will review the relevant record and, where necessary, verify the information against the underlying source footage stored within the VMS or associated analytics outputs generated through the analytics tool. If the review determines that the information in the record is inaccurate or incomplete, the Governance Partner will correct the record where feasible or attach an annotation documenting the correction or the individual's request or will direct the appropriate Operational Partner to do so.

Where the record reflects an interpretation, observation, or professional assessment made by an operator or authorized personnel at the time the record was created, the record may not be altered if the information accurately reflects the original observation or decision-making context. In these circumstances, the Governance Partner will add an annotation to the record noting the individual's request for correction and any relevant clarification, ensuring that future users of the record are aware of the individual's position while preserving the integrity of the original administrative record.

8.3.3 Notification Following Correction or Annotation

Where a correction or annotation is made, the Governance or Operational Partner will take reasonable steps to notify any Participant Organizations to which the information was previously disclosed, where such notification is necessary to ensure consistent records across participating organizations.

Notification obligations may include:

- informing relevant Participant Organizations that a correction or annotation has been made;
- providing updated information or contextual clarification where appropriate; and
- ensuring that partner organizations update any related administrative records under their control.

These notification steps are undertaken in accordance with applicable legal obligations and the governance provisions of the Information Sharing Agreement.

8.3.4 Coordination Among Program Partners

As the Common Program involves multiple partner organizations participating in operational coordination, correction and annotation processes require coordination across the governance structure established for the Common Program.

To support consistent record management:

- Each Participant Organization remains responsible for correcting or annotating records under its custody or control.
- Where records have been shared with partner organizations for operational purposes, the originating organization will notify relevant partners if a correction or annotation affects information previously disclosed.
- Program governance bodies and designated privacy contacts may coordinate responses to complex correction requests that involve multiple organizations or shared operational records.

This coordinated approach ensures that correction requests are handled transparently and consistently while respecting each partner organization's legal responsibilities for records under its custody or control.

In some circumstances, the VPD may have exported records associated with the Common Program that are now held by or disclosed to other law enforcement agencies for operational or investigative purposes. Where video footage or related records have been exported and are subsequently held by a law enforcement agency as part of an investigation or enforcement activity, those records fall under the custody or control of that agency.

In such cases, access requests relating to those records may be transferred to the appropriate law enforcement body in accordance with applicable access to information legislation. Where appropriate, participating organizations may coordinate with the VPD and other law enforcement partners to ensure that requests are directed to the public body best positioned to respond, while maintaining compliance with legislative requirements governing custody, control, and disclosure of records.

8.4 Access to Information Requests

The Governance Partners recognize that records generated through the operation of the camera network may be subject to requests under applicable access to information legislation. Participant Organizations remain responsible for responding to requests for access to records under their custody or control in accordance with the FIPPA. The following processes supports the identification, retrieval, and coordination of responsive records where information relating to the Common Program may involve multiple Participant Organizations.

8.4.1 FOI Request Handling Model

Access to information requests relating to Common Program records will be processed or coordinated by the Governance Partner responsible for the Operational Partner who receives the request. That Operational Partner is responsible for managing their own requests, identifying responsive records within its custody or control, and applying any applicable legislative exceptions or severing requirements.

Where responsive records include video footage, retrieval and export of the footage will occur through authorized system administrators of the Governance Partner in accordance with established operational procedures. Extracted records will be provided to the responsible access and privacy office for review, severed where required, and response to the applicant.

Automated analytics outputs generated by the system are not maintained as standalone disclosure datasets. Any disclosure of analytics information will rely on the underlying video footage and will be assessed within the context of the applicable legislative authority.

8.4.2 Coordination Among Participating Public Bodies

To support consistent and efficient handling of access requests:

- Each participating public body remains responsible for responding to requests for records under its custody or control.

- Control of video footage remains with the Governance Partners alone, even if footage has been shared with an Operational Partner under section 7.4.5.
- Where an access request received by one organization may involve records held by another Program partner, the receiving organization may notify the relevant partner organization to determine whether additional responsive records exist.
- Where an access request is received by an Operational Partner that involve records under the control of a Governance Partner, the Operational Partner must transfer that access request to the Governance Partner under FIPPA section 11.
- Program governance agreements establish operational contacts within each participating organization to facilitate efficient identification and retrieval of records related to the Program.

This coordination helps ensure that access requests are processed in accordance with legislative requirements while recognizing the distributed nature of records generated through the Program.

8.4.3 Retrieval and Record Identification

Video footage and associated records are stored within the VMS' technical systems and may be retrieved using system search tools and audit capabilities. Authorized personnel may use system metadata, timestamps, camera identifiers, or other operational information to identify relevant footage or associated records.

Where necessary to locate responsive records, system administrators may conduct targeted searches within the video management and analytics systems while maintaining system audit logs documenting the retrieval activity.

8.4.4 Program Support for FOI Compliance

The Common Program's technical and governance design supports access to information compliance through:

- secure storage of video records within the video management system;
- audit logging of access, retrieval, and export activities;
- defined operational procedures for authorized footage extraction; and
- governance coordination mechanisms among participating public bodies.

These measures assist Participant Organizations in identifying responsive records and responding to access requests in a timely and accountable manner.

8.5 Access, Transparency, and Individual Rights Risk Assessment

This section gives a narrative overview of the risks and mitigation strategies. A simplified table-version of this information is found in the Risk Register, located in Annex D.

8.5.1 Transparency and Public Awareness

The Common Program recognizes that transparency is an important safeguard in programs involving the video collection of personal information in public spaces. Individuals should be reasonably informed when they are entering areas subject to video monitoring so they can understand the purpose of the **[**collection and the public bodies responsible for its operation.

Because cameras may capture individuals who are not directly interacting with program personnel, there is a risk that individuals may not be aware that video monitoring] is occurring or may not understand the purposes for which the information is collected and used. Lack of transparency can undermine public trust and may limit individuals' ability to exercise their rights under applicable access and privacy legislation.

To mitigate these risks, the Common Program implements a signage and transparency framework designed to provide clear notice to members of the public. Signage is placed in visible locations within camera coverage areas to inform individuals that video collection is in operation. These notices include information indicating that video monitoring is occurring, the general purpose of the situational awareness, and contact information for the responsible public body or privacy office. Examples are covered above in section 8.1.

In addition to physical signage, the Common Program supports transparency through publicly available information about the program. Governance Partners maintain publicly accessible information describing the program's purpose, the types of technologies used, and the applicable governance and privacy protections. This information may be published through the City of Vancouver's FWC26 websites or other public communication channels.

These measures help ensure that individuals are provided with reasonable notice of situational awareness activities and information about how their personal information may be collected, used, and disclosed within the program.

8.5.2 Signage Effectiveness and Operational Limitations

While signage and public communication measures support transparency, certain operational limitations may affect the ability to notify every individual who enters an area monitored by cameras. For example, individuals may enter camera coverage areas from multiple directions, may not notice signage due to environmental conditions or crowd density, or may pass through areas quickly without observing posted notices.

To mitigate these limitations, signage is designed to be reasonably visible and placed at locations where individuals are likely to enter monitored areas. Program partners may also supplement signage with additional transparency measures, such as publicly available program descriptions and privacy contact information, to ensure that individuals can obtain further information if desired.

The objective of these measures is to provide reasonable notice of video collection activities consistent with applicable privacy legislation while recognizing that it may not be feasible to ensure that every individual observes signage in dynamic public environments.

8.5.3 Transparency and Accountability Measures

Transparency about situational awareness practices also supports accountability and oversight. Clear public communication regarding the existence and purpose of the camera network helps ensure that members of the public understand how personal information is collected and how privacy risks are managed.

The Common Program therefore incorporates transparency measures into its governance framework, including the publication of program information and the availability of designated privacy contacts within participating organizations. These mechanisms allow individuals to seek additional information about the program, raise concerns, or exercise their rights under applicable access and privacy legislation.

Together, signage, public information resources, and governance transparency measures help support public awareness while balancing the operational needs of the program**.**

8.5.4 Accuracy and Interpretation Risks

The Common Program relies on video footage and analytics outputs to support operational awareness and coordination among authorized personnel. While these technologies can assist in identifying events or relevant video segments, there is a risk that automated analytics outputs or visual information could be misinterpreted or relied upon without appropriate verification. Video analytics tools may generate false positives, incomplete detections, or classification errors due to environmental conditions, camera angles, lighting, weather, crowd density, or other contextual factors. In addition, video footage itself may present only a partial view of an event and may be susceptible to misinterpretation if reviewed without adequate context.

To mitigate these risks, the Common Program implements a human verification requirement whereby automated analytics outputs are treated strictly as decision-support tools. Operational personnel are required to review the underlying video footage before relying on analytics alerts, classifications, or search results for operational coordination or investigative purposes. Analytics outputs are therefore not used as authoritative records in isolation, and any operational interpretation must be validated against the source footage maintained within the VMS.

Operator training further mitigates the risk of misinterpretation. Personnel authorized to access the system receive training on the capabilities and limitations of video analytics technologies, the appropriate interpretation of visual information, and procedures for confirming events through manual review of footage. Training also includes instruction on the privacy obligations applicable to the Common Program and the use of personal information in accordance with FIPPA and program governance policies.

Additional safeguards include contextual interpretation guidance requiring operators to assess video footage within the broader operational context and avoid drawing conclusions based solely on automated classifications or isolated frames. These procedures help ensure that operational decisions are supported by verified information rather than automated system outputs alone.

The program also incorporates technical and governance controls to support system reliability. Cameras and analytics systems are configured and maintained in accordance with vendor specifications and operational requirements, and technical administrators periodically review

system performance to identify and address potential issues affecting video quality or analytics performance.

The Common Program also prohibits the use of facial recognition technology capabilities. This restriction reduces the risk of inaccurate or biased identification of individuals and reflects the program's commitment to minimizing privacy risks associated with automated identification technologies.

Finally, audit logging within the VMS records access to video footage and the retrieval of clips. These audit records enable monitoring of system use and support accountability where questions arise regarding the interpretation or operational use of information derived from the system.

Together, these measures support the reasonable accuracy of information derived from the system while recognizing the inherent limitations of video-based technologies.

8.5.5 Data Integrity and Correction Risks

As video systems capture visual records of events as they occur, the ability to "correct" the underlying record is inherently limited. There is a potential risk that individuals may believe the video footage itself inaccurately represents events or may dispute interpretations recorded in associated administrative records, such as incident summaries or operational notes.

To preserve evidentiary integrity and maintain reliable records management practices, the Common Program does not alter original video recordings once captured. Video footage maintained within the VMS is preserved as an authentic, time-stamped record of events as recorded by the system at the time of capture. Altering original recordings could compromise the authenticity of the record, undermine evidentiary reliability, and interfere with system audit trails, retention controls, and chain-of-custody mechanisms.

Instead, correction processes focus on associated metadata, contextual descriptions, and administrative records generated through the operation of the system. Where individuals submit correction requests under applicable access and privacy legislation, the responsible Governance or Operational Partner reviews the relevant records and verifies the information against the underlying source footage and associated system logs.

If the request is determined to be justified, the responsible organization will correct the relevant metadata or administrative record where technically feasible. Where a correction cannot be made—such as where the record reflects an observation or interpretation recorded at the time of an event—the organization will attach an annotation documenting the individual's position regarding the accuracy of the information. This approach ensures that future users of the record are aware of the individual's request while preserving the integrity of the original record.

Because the Common Program involves multiple partner organizations, correction and annotation processes may require coordination among participating public bodies. Each organization remains responsible for records under its custody or control, while governance procedures support notification and coordination where corrections affect information previously disclosed to partner organizations.

8.5.6 Access to Information and Records Coordination Risks

Records generated through the operation of the camera network may be subject to requests under access to information legislation. Given the distributed nature of the Common Program and the involvement of multiple partner organizations, there is a risk that access requests could be delayed or complicated if responsibilities for records custody and control are unclear or if responsive records are held across multiple participating organizations.

The program mitigates this risk through clearly defined governance and operational procedures for handling access requests. Each participating public body remains responsible for responding to requests for records under its custody or control in accordance with FIPPA. Governance Partners maintain control of video footage stored within the VMS and provide authorized technical support for retrieval and export of responsive footage where required for access requests.

Where an access request received by one organization involves records under the control of another participating public body, established procedures allow the request to be transferred or coordinated in accordance with FIPPA requirements. Operational contacts within participating organizations facilitate coordination to identify responsive records and ensure that requests are directed to the public body best positioned to respond.

The system’s technical design also supports access compliance by maintaining secure storage of video footage within the VMS, providing search capabilities to locate relevant records, and generating audit logs documenting retrieval activities. These mechanisms assist participating organizations in identifying responsive records while maintaining accountability and transparency regarding system access and use.

PART 9 – RETENTION AND DISPOSITION

9.1 Program-Level Retention Principles

The Common Program adopts a data minimization and proportionality-based approach to the retention of personal information collected through the Common Program]. Retention periods are designed to balance operational utility with privacy protection, ensuring that personal information is not retained longer than necessary to fulfill authorized purposes.

9.1.1 Minimum Retention Standards

Video footage collected through the Common Program is retained for a defined baseline period sufficient to support operational review, incident response, and investigative follow-up. This baseline retention period is:

- Limited to the shortest duration necessary to enable authorized personnel to identify, review, and act on relevant events
- Established consistently across Governance Partners unless a justified operational need supports variation
- Supported by system-level controls that enforce automated deletion at the end of the retention period

Where no incident, investigation, or authorized use has been identified within the retention window, footage is automatically and irreversibly deleted.

Restrictions on Extended Retention

Retention beyond the standard period is permitted only where:

- The footage has been flagged for a specific, documented purpose, such as an active investigation, legal requirement, or authorized disclosure
- The extension is approved in accordance with defined governance procedures and role-based authorities
- The continued retention is necessary and proportionate to the identified purpose

Extended retention is subject to the following controls:

- Time-limited extensions with defined review intervals
- Documentation of the rationale for continued retention
- Periodic verification to confirm ongoing necessity

Under no circumstances is video footage retained indefinitely. All extended retention must align with applicable legal authorities, including requirements under *FIPPA*, and applicable records management obligations.

9.2 Partner-Specific Retention

Each Participant Organization is responsible for ensuring that video records are:

- Reflected in their Directory of Records (or equivalent records inventory). The City and VPD both have a common established records retention period of thirty days for video recording records.
- Classified in accordance with applicable records schedules and retention bylaws or policies
- Managed in a manner consistent with both the Common Program requirements and the partner's internal records management framework

Where discrepancies arise between program-level retention standards and partner-specific records schedules, the more privacy-protective approach will be applied unless legal obligations require otherwise.

However, as discussed above, the City does not foresee disclosing personal information to Operational Partners. The VPD will limit disclosure to other law enforcement agencies only in the event of a verified investigation.

9.3 Secure Disposal

The Common Program implements secure, auditable, and irreversible disposal processes to ensure that personal information is appropriately destroyed at the end of its retention period.

9.3.1 Disposal Methods

Video data is stored within an on-premises environment and is disposed of using technical methods designed to prevent reconstruction or recovery. These methods include:

- Automated deletion protocols embedded within the Video Management System (VMS)
- Overwriting or secure wiping of storage media in accordance with industry standards
- Controlled disposal of physical storage components, where applicable, using approved destruction methods

All disposal processes are designed to ensure that personal information cannot be reconstructed, accessed, or retrieved following deletion.

9.3.2 Verification and Documentation

The Common Program incorporates mechanisms to verify and document disposal activities, including:

- System-generated logs confirming deletion events
- Audit capabilities to track retention and deletion actions
- Periodic reviews to confirm that retention limits are being enforced as configured

Authorized personnel responsible for system administration and oversight are accountable for ensuring that disposal processes function as intended and that any anomalies are identified and addressed.

Where required, disposal activities may be subject to internal audit or external review to demonstrate compliance with applicable legal and policy requirements.

PART 10 – PRIVACY RISK ASSESSMENT

As part of this Privacy Impact Assessment, potential risks to personal information associated with the program and supporting technology have been identified and evaluated. The purpose of the risk assessment is to determine whether personal information is adequately protected through appropriate administrative, technical, and operational safeguards. This assessment considered risks that could arise from the collection, use, disclosure, storage, or access to personal information within the system, including risks related to system access controls, data exports, monitoring activities, governance processes, and information security safeguards.

Potential risks were identified through a review of the system architecture, operational workflows, user access roles, data handling practices, and applicable legislative and policy requirements. Risks were also considered in relation to common privacy vulnerabilities associated with systems that store or process personal information, including risks related to unauthorized access, inappropriate use, excessive disclosure, or insufficient oversight. Each identified risk is documented in the risk register contained in Appendix E: Privacy Risk Register.

10.1 Risk Scoring Approach

Each risk is evaluated using a qualitative risk scoring model that considers both the likelihood that a risk event may occur, and the potential impact should the event occur. Likelihood and impact are each scored on a scale from 1 to 5, where:

10.1.1 Likelihood Score Description

1	Very unlikely to occur
2	Unlikely
3	Possible
4	Likely
5	Very Likely

10.1.2 Impact Score Description

1	Minimal privacy impact
2	Low impact affecting limited information or individuals
3	Moderate impact affecting identifiable individuals or operational processes
4	Significant impact, including unauthorized disclosure of personal information
5	Severe impact, including widespread disclosure or serious harm to individuals or common program participants

The Unmitigated Risk Score is calculated by multiplying the likelihood score by the impact score: **Unmitigated Risk Score = Likelihood × Impact**. This score reflects the level of risk before any safeguards or mitigation measures are applied.

Risk levels correspond to the following matrix.

Likelihood ↓ / Impact →	1 Minimal	2 Low	3 Moderate	4 Significant	5 Severe
5 Very Likely	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Very Unlikely	1	2	3	4	5

10.1.3 Mitigation measures

For each identified risk, mitigation measures were assessed to determine whether administrative, technical, or procedural safeguards reduce the likelihood of the risk occurring or reduce the potential impact should it occur.

Mitigation measures may include, for example:

- role-based access controls,
- authentication and authorization safeguards,
- system logging and monitoring,
- export controls and operational procedures,
- governance and oversight mechanisms, and
- records management and retention controls.

Where safeguards are already implemented within the system or program design, these controls are considered in the evaluation of residual risk.

10.1.4 Residual Risk

The Residual Risk Score reflects the level of risk remaining after mitigation measures and safeguards are applied.

Residual risk represents the risk that remains after the following have been considered:

- technical safeguards,
- administrative controls,
- operational policies, and
- governance mechanisms

Residual risk scores help determine whether risks are considered acceptable within the operational context of the program or whether additional mitigation measures may be required.

The following matrix illustrates how Residual Risk Scores are interpreted after mitigation measures have been applied. The matrix is based on the Likelihood × Impact scoring model described above. Residual risk colours are used within the Privacy Risk Register to visually identify the relative level of remaining privacy risk after safeguards have been considered.

10.1.5 Residual Risk Colour Definitions

Residual Risk Score	Risk Level	Colour Code	Description
1–4	Low	Green	Risk is minimal and adequately controlled through existing safeguards. No additional mitigation is typically required beyond routine monitoring.
5–9	Moderate	Yellow	Risk is manageable but requires continued oversight to ensure safeguards remain effective. Additional mitigation may be considered if operationally feasible.
10–16	High	Orange	Risk requires active management and strong safeguards. Program leads should ensure controls are consistently implemented and monitored.
17–25	Very High	Red	Risk may require additional mitigation measures or governance oversight before the program proceeds or continues operation.

10.2 Risk Register

A detailed register of identified risks, including likelihood scores, impact scores, mitigation measures, and residual risk assessments, is provided in Appendix E: Privacy Risk Register.

Overall, the safeguards described in this PIA are intended to reduce identified risks to a level that is proportionate to the operational objectives of the program while ensuring that personal information is protected through reasonable security arrangements.

10.3 Collaborative Risk Assessment

The privacy risks and mitigation measures described in this assessment were developed through consultation with program leads, technical system administrators, and privacy professionals responsible for privacy compliance and information security. This collaborative approach ensures that the risk analysis reflects both the operational realities of the program and the safeguards implemented within the system, and that privacy considerations have been integrated into the program's governance, design, and ongoing oversight processes.

10.3.1 Acceptance of Residual Risk

The signatories to this Privacy Impact Assessment acknowledge the residual risks identified in this assessment and confirm that the safeguards and mitigation measures described in this document will be implemented and maintained. Based on the controls in place, the remaining risks are considered proportionate to the operational objectives of the program and acceptable within the organization's privacy and security governance framework.

PART 11 – CHANGE MANAGEMENT AND OVERSIGHT

11.1 PIA Update Triggers

Given the time-limited nature of the Common Program, formal PIA updates will be limited to changes that materially alter the privacy risk profile within the operational period of June 7 to July 19, 2026.

11.1.1 Material Changes

A targeted PIA update or documented addendum will be completed where:

- New technologies or analytics capabilities are introduced that were not assessed in this PIA
- There is a change to the approved purposes or scope of the program
- Data flows change in a manner that introduces new uses or disclosures of personal information
- Hosting, network architecture, or access models are materially modified

Minor operational adjustments that do not affect the nature, scope, or sensitivity of personal information will be documented through internal change logs rather than formal PIA revisions.

11.1.2 New Partners or Zones

Due to the defined program scope and timeline:

- The onboarding of new partners or expansion into new zones will be exceptional and subject to documented privacy review prior to implementation
- Where approved, changes will be captured through annex updates rather than reopening the full PIA, unless risk levels materially change
- No expansion will proceed without confirming alignment with the original legal authority, purpose, and safeguards.

11.1.3 BC OIPC Consultations

Engagement with the Office of the Information and Privacy Commissioner for British Columbia will be limited to circumstances where:

- A material and unanticipated privacy risk arises; or
- Program changes introduce novel or higher-risk processing not previously assessed.

Where consultation occurs, outcomes will be documented and incorporated into program controls for the remainder of the operational period.

11.2 Ongoing Privacy Monitoring

Privacy oversight during the program will be risk-based, proportionate, and focused on ensuring compliance throughout the limited operational window.

11.2.1 Audits and Reviews

Monitoring activities will include:

- Periodic reviews of access logs and footage retrieval to confirm authorized use;
- Verification of role-based access controls and user permissions, and data extraction for investigations;
- Spot checks of compliance with retention limits and secure disposal timelines; and
- Targeted reviews in response to incidents, complaints, or identified anomalies.

Given the short duration, audits will prioritize real-time or near-real-time assurance over extensive retrospective review.

11.2.2 Compliance Reporting

The program will maintain concise but complete records to demonstrate compliance with the *Freedom of Information and Protection of Privacy Act* (British Columbia), including:

- Documentation of access and use of video data;
- Tracking of any privacy incidents and mitigation actions; and
- Summary reporting to the Governance Participants.

Reporting will be structured to support both operational oversight and end-of-program accountability.

11.3 Partner Exit and Off-Boarding

As the program is time-limited, off-boarding requirements apply both to individual partner withdrawal (if any) and to full program decommissioning at the conclusion of the six-month period.

11.3.1 Data Handling Upon Exit

Upon partner exit or program conclusion:

- Access to systems will be promptly revoked;
- Participating partners will not retain copies of video footage or analytics outputs unless authorized under applicable law;
- All records will be retained or disposed of in accordance with approved retention schedules and legal requirements; and
- Where required, data will be securely returned or destroyed, with appropriate confirmation.

End-of-program data handling will prioritize timely disposal and avoidance of unnecessary continued retention.

11.3.2 Residual Access Controls

To prevent unauthorized access following exit or decommissioning:

- All user accounts will be disabled or removed;
- Credentials and physical access permissions will be revoked;
- Shared system access points and integrations will be reviewed and decommissioned; and
- Audit logs will be reviewed to confirm termination of access and identify any anomalies.

A final access validation will be conducted at program close to ensure no residual access pathways remain.

PART 12 – PUBLIC TRANSPARENCY AND ACCOUNTABILITY

12.1 Public-Facing Transparency Measures

Public-facing transparency will be supported through clear, accessible descriptions of the program, including its purpose, participating partners, and the general nature of technologies and monitoring activities in use. These descriptions will be made available through appropriate public channels (e.g., websites and public notices) and will align with the collection notification approach outlined above.

Accountability will be reinforced through defined governance structures, including identified program leads, documented roles and responsibilities, and oversight mechanisms embedded within the common program agreement. These measures are intended to ensure that program activities remain aligned with applicable legal requirements and approved purposes.

12.2 Complaints and Oversight

Individuals may raise questions or complaints regarding the program through established access and privacy channels of the relevant public body. Complaints will be reviewed and addressed in accordance with existing policies and legislative requirements, including escalation where appropriate.

The program is currently subject to engagement with the regulator through review of the Privacy Impact Assessment and the common program agreement. Ongoing cooperation with the regulator will be maintained, including responding to inquiries, supporting any reviews or investigations, and implementing recommendations as appropriate.

PART 13 – CONCLUSIONS AND CONDITIONS

13.1 Summary of Privacy Findings

The proposed program involves the deployment of camera technologies across a range of environments, including controlled facilities, semi-public access points, and fully public areas such as transit corridors, nightlife districts, and approach routes to event zones. As a result, the privacy risk profile varies by context, with the highest sensitivity arising in public-facing environments characterized by high variability, mixed-use activity, and the presence of individuals who are not participating in the event. In these areas, there is an increased likelihood of incidental collection, including the capture of individuals in sensitive but lawful contexts (e.g., nightlife activity, demonstrations, or interactions involving vulnerable populations). Movement patterns are less predictable, and individuals may enter monitored spaces without direct awareness of the program, creating additional challenges for ensuring meaningful notice and limiting over-collection.

Public-area deployments also introduce heightened considerations related to Charter-protected activities, including freedom of expression and peaceful assembly. The presence of cameras in areas where demonstrations or gatherings may occur raises the potential for both actual and perceived impacts on these freedoms. While the system is not designed or intended to identify individuals or monitor participation in lawful activities, the possibility of perceived video monitoring in these contexts contributes to an elevated level of scrutiny and requires careful design and governance to ensure proportionality.

In addition to fully public environments, the program includes deployment at the exterior of hotels and a convention centre, which introduces a distinct set of contextual privacy considerations. Although these areas are publicly accessible, they are associated with heightened expectations of discretion, particularly for hotel guests, business travellers, and individuals attending conferences or meetings. Camera coverage at entrances and drop-off areas may incidentally capture patterns of arrival, departure, or association, including participation in specific events or gatherings. This creates a moderate but contextually elevated sensitivity, reflecting the intersection of public visibility and private or commercial activity.

Across all zones, privacy risks are mitigated through a combination of purpose limitation, non-targeted and overt camera deployment, and strong governance controls. Camera use is restricted to situational awareness, safety, and operational coordination, and the program explicitly prohibits identification-based uses, including facial recognition, or the monitoring of individuals engaged in lawful expressive activity. Additional safeguards include data minimization, time-limited retention, strict access and disclosure controls, and comprehensive auditability mechanisms. The program is also explicitly time-limited, with defined sunset provisions and decommissioning requirements to prevent function creep or normalization beyond the event context.

A layered transparency approach—including prominent signage, public-facing materials, and ongoing engagement with the regulator—supports accountability and helps ensure that individuals are informed of the program. Particular attention has been given to clearly delineating authority and system boundaries, including the separation of program-operated

cameras from privately managed surveillance systems (e.g., within hotels or the convention centre), to avoid ambiguity in accountability.

Residual privacy risks remain inherent to the use of video monitoring technologies in public and semi-public environments, particularly in relation to incidental collection, perception of surveillance, and contextual sensitivity of certain activities or locations. However, these risks have been assessed as proportionate to the program's objectives and are mitigated to a level that aligns with applicable privacy legislation and reflects appropriate consideration of Charter values. Overall, the program demonstrates a measured, context-sensitive approach that balances operational requirements with the protection of individual privacy.

Key privacy considerations include:

- The collection of personal information through video monitoring in public and semi-public spaces;
- The coordination of multiple public and private sector partners, requiring strong governance and consistent application of privacy controls;
- The potential for function creep, particularly in relation to analytics;
- Risks associated with access control, data handling, and system security, including both cyber and physical dimensions; and
- The need to ensure meaningful transparency to individuals entering monitored zones.

The PIA finds that:

- The Program has a clearly defined and time-limited purpose tied to event safety, security, and situational awareness;
- Data minimization principles have been incorporated through camera positioning, limited analytics use, and restrictions on collection scope;
- Role-based access controls, audit logging, and governance structures provide a strong foundation for accountability;
- Retention and disposal practices are defined at a program level and further specified through partner-specific requirements;
- A layered transparency approach (including zone-based signage and public materials) supports openness and public awareness; and
- The Program includes active engagement with the BC OIPC and reflects alignment with applicable legislative requirements under FIPPA.

Overall, the Program introduces elevated but controlled privacy risks due to the use of distributed camera infrastructure, centralized monitoring, multi-partner data sharing, and limited analytics capabilities within a public environment.

13.2 Conditions of Approval

Implementation of the Program should be contingent on the following conditions:

Governance and Accountability

- Finalization and execution of a common program agreement clearly distinguishing governance partners from operational participants; and
- Confirmation of decision-making authority, accountability structures, and escalation pathways.

Transparency and Public Notice

- Deployment of standardized and zone-specific collection notices prior to program activation; and
- Publication of public-facing program descriptions, including purpose, scope, and contact information.

Access and Use Controls

- Full implementation of role-based access controls (RBAC) aligned to defined user roles;
- Activation of comprehensive audit logging, including access to and export of footage; and
- Enforcement of strict limitations on use, including prohibition of unauthorized analytics or secondary use.

Retention and Disposal

- Confirmation of program-level retention limits; and
- Implementation of secure and verifiable disposal processes at the conclusion of retention periods and at program end.

Security Safeguards

- Validation of physical, technical, and administrative safeguards, including:

Training and Operational Readiness

- Completion of mandatory privacy and security training for all authorized users prior to system access; and
- Distribution of operational guidance and acceptable use expectations.

Regulatory Engagement

- Continued engagement with the BC OIPC through review of the PIA and associated program agreements; and
- Review, due consideration, and incorporation of any regulatory feedback or required modifications prior to activation.

Time-Limited Controls

- Enforcement of a defined program end date, with no continuation or expansion without further review and approval; and
- Confirmation of decommissioning procedures, including data disposition and system shutdown.

PART 14 – SIGNATURES AND COMMENTS

City of Vancouver			
Name	Position	Signature	Date
Sandra Singh, Deputy City Manager	Program Authority	s.15(1), s.22(1)	26/05/26
Tadhg Healy, Chief Technology Officer	Technology Authority		25/05/26
Francie Connell, Director Legal Services	Legal		26/05/26

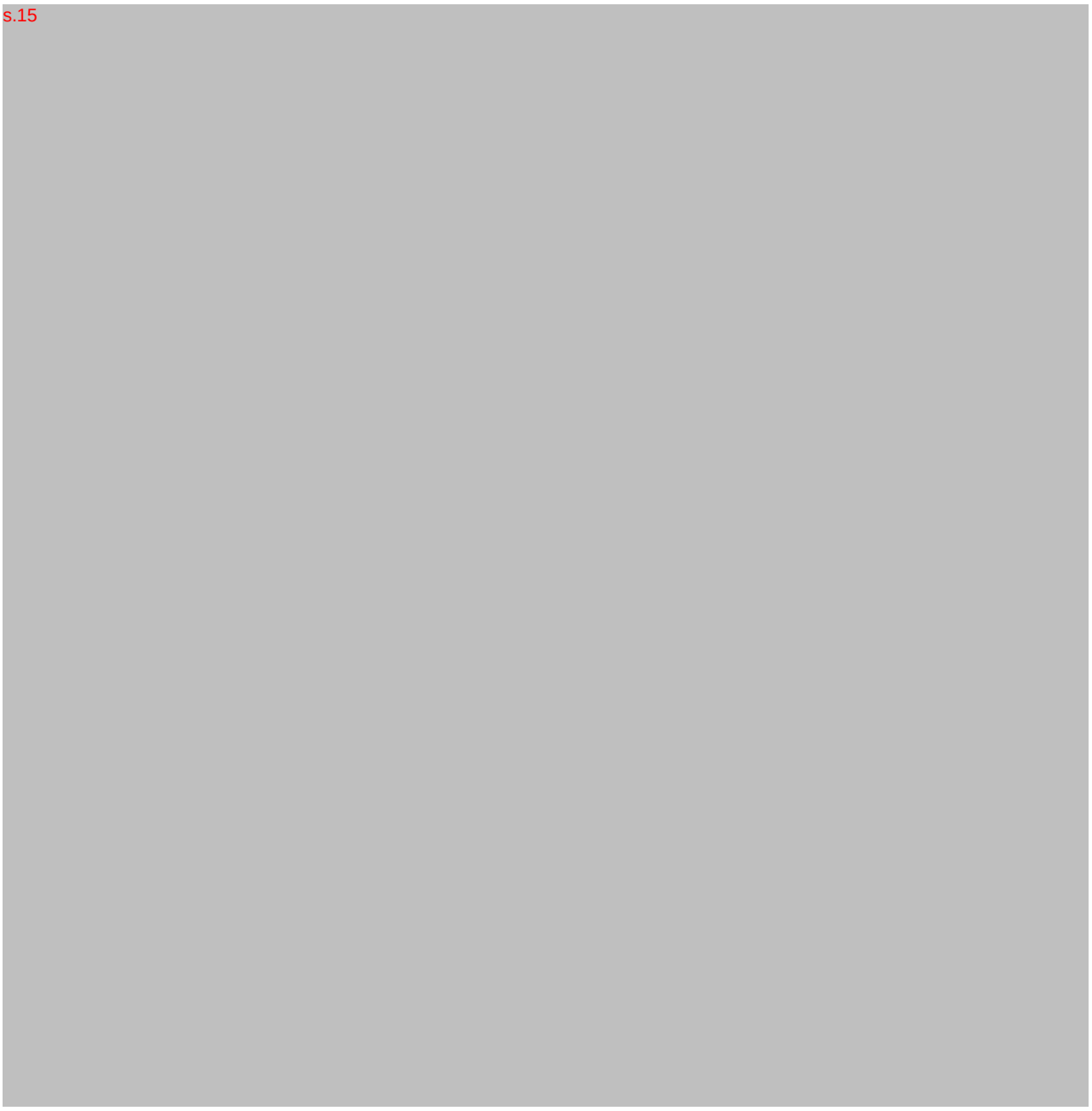
Vancouver Policy Department			
Name	Position	Signature	Date
Deputy Chief Constable Don Chapman, Strategy & Innovation Division	Program Authority	s.15(1), s.22(1)	26/05/26
Darrin Hurwitz, Senior Legal Counsel	Legal		

ANNEXES AND APPENDICIES

Annex A: Zone-Specific Privacy Analysis (Zones 1–6)

Camera deployment varies by zone and is designed to reflect the operational character of each environment, including controlled training facilities, controlled-entry event spaces, public approach corridors, entertainment streets, and hotel-adjacent access areas. Across these zones, cameras are deployed in a manner intended to support specific event-related public safety, security, and operational coordination purposes, while limiting collection to what is reasonably necessary in the circumstances.

s.15



s.15 [redacted]

No camera placement is intended to monitor washrooms, change rooms, treatment or medical areas, private offices, or other locations where individuals have a heightened expectation of privacy. Where there is any potential for incidental capture of non-relevant or privacy-sensitive space, mitigation measures such as angle adjustment, restricted fields of view, and privacy masking are used to support compliance with data minimization and proportionality principles.

A camera audit will be conducted to ensure camera installation complies with these principles outlined in the Annex.

Zone 1: Killarney Training Facility

The Killarney Training Facility is located at Killarney Park, in southeastern Vancouver. The zone covers the training facility's parking lots, entrances and exits, and pitch. This is an area restricted to the public, for practice by teams playing later in the weeks at BC Place.

A1.1 Zone Characteristics

A1.1.1 Density of Individuals
The zone experiences moderate and episodic density. Peak occupancy occurs during scheduled team practices or events, where participants and limited support personnel are present. Outside of these periods, the area is largely unoccupied. Spectator presence is minimal or absent given the controlled nature of the facility.

A1.1.2 Predictability of Movement
Movement within the zone is highly predictable and structured. Individuals primarily follow established pathways between parking areas, facility entrances/exits, and the playing surface. Activities on the pitch are organized and confined to defined practice or training patterns.

A1.1.3 Presence of Vulnerable Populations
Access is mediated through team, organizational, or supervisory structures, reducing the likelihood of unaccompanied or incidental presence of minors or vulnerable populations.

A1.1.4 Duration of Individual Presence
Individuals are present for defined and time-limited periods, generally corresponding to scheduled practices or training sessions. Typical durations range from short transitions (e.g., arrival/departure through parking and entry points) to longer but still bounded periods (e.g., duration of a practice session).

A1.1.5 Public vs. Semi-Public vs. Controlled Environment
This zone is a controlled-access environment that is not open to the general public. Access is restricted to authorized individuals (e.g., athletes, coaches, staff). While certain areas (e.g., parking lots, entrances/exits) may functionally resemble semi-public spaces, overall access is governed and limited. s.15 [redacted]
s.15 [redacted]
s.15 [redacted]

A1.1.6 Camera Coverage Context

s.15 s.15 . There is no monitoring of private interior spaces (e.g., change rooms), s.15 s.15

A1.2 Camera Placement and Coverage

CCTV deployment at training sites is focused primarily s.15 s.15 s.15 s.15 . The scope of monitoring is deliberately limited, and generalized behavioral observation is avoided. These measures ensure that CCTV use remains aligned with its intended purpose of supporting safety and security without introducing unnecessary privacy intrusion.

Zone 2: UBC National Soccer Training Centre

The UBC National Soccer Training Centre is located at the University of British Columbia. The zone covers the training facility's parking lots, entrances and exits, and pitch. This is an area restricted to the public, for practice by teams playing later in the weeks at BC Place.

A2.1 Zone Characteristics

A2.1.1 Density of Individuals

The zone experiences variable density, ranging from low to moderate during routine practices. Practices may include athletes, coaching staff, officials, and up to 300 spectators, resulting in increased concentration of individuals in both the stands and surrounding areas (e.g., entrances, exits, and parking).

A2.1.2 Predictability of Movement

Movement within the zone is generally structured but becomes less predictable during events. During practices, movement follows established patterns between parking areas, entrances/exits, and the playing surface. During practice, additional and less predictable movement patterns emerge, including spectator circulation, congregation areas, and intermittent surges at entry and exit points.

A2.1.3 Presence of Vulnerable Populations

Access is mediated through team, organizational, or supervisory structures, reducing the likelihood of unaccompanied or incidental presence of minors or vulnerable populations. The presence of minors and broader public attendees during games introduces a higher likelihood of vulnerable individuals compared to controlled training-only environments.

A2.1.4 Duration of Individual Presence

Individuals are present for defined but variable durations. Practice participants may only remain for the duration of scheduled sessions. All spectators and event attendees must leave with their team at the end of the practice period.

A2.1.5 Public vs. Semi-Public vs. Controlled Environment

This zone operates as a hybrid environment:

- *Controlled access* during team practices or restricted training periods (limited to authorized participants), and
- *Semi-public access* during practice events, where invited spectators may attend.

A2.1.6 Camera Coverage Context

s.15 s.15 s.15 There is no monitoring of private interior spaces (e.g., change rooms), and coverage remains aligned with safety, security, and event coordination purposes within a dynamic campus setting.

A2.2 Zone-Specific Camera Deployment Overview

This zone is a controlled-access environment that is not open to the general public. Access is restricted to authorized individuals (e.g., athletes, coaches, staff). While certain areas (e.g., parking lots, entrances/exits) may functionally resemble semi-public spaces, overall access is governed and limited. s.15 s.15

Zone 3: FanFest (PNE)

FanFest will be held in Hastings Park adjacent to the Pacific National Exhibition Grounds (PNE). The zone will be open to the public, with controlled entrances to limit overcrowding. The zone covers the park's entrances and exits. Ticketed events are semi-public when using the Pacific Coliseum.

A3.1 Zone Characteristics

A3.1.1 Density of Individuals
The zone experiences consistently high density, particularly during peak event periods. Large volumes of attendees are expected within confined areas of the park, including queues, viewing zones, vendor areas, and circulation pathways. Density may fluctuate throughout the day but generally remains elevated relative to non-event environments.

A3.1.2 Predictability of Movement
Movement within the zone is moderately predictable but highly dynamic. While entry and exit points, queueing areas, and primary pathways are structured, individual movement within the festival space is fluid and crowd-driven, with congregation around stages, attractions, and vendors. Surges and bottlenecks may occur at peak times.

A3.1.3 Presence of Vulnerable Populations
The zone includes a broad cross-section of the public, including children, youth, and other potentially vulnerable individuals. The event environment increases the likelihood of vulnerable persons being present in large numbers, sometimes within dense crowds and dynamic conditions.

A3.1.4 Duration of Individual Presence
Individuals are present for extended but variable durations, ranging from short visits to multi-hour attendance over the course of the event. Unlike transit-style environments,

individuals are more likely to remain within the zone for prolonged periods, increasing the potential for repeated or continuous observation.

A3.1.5 Public vs. Semi-Public vs. Controlled Environment
This zone is best characterized as a controlled-entry, public environment, with some events occurring in a semi-public environment at the Pacific Coliseum:

- Access to the overall FanFest area is public through controlled entry points, with crowd number supervision by security staff.
- Access to the Pacific Coliseum restricted through ticketing and screening mechanisms, and
- Once inside, the space functions similarly to a public gathering environment, with relatively free movement within the defined perimeter.

As such, the zone combines elements of controlled access with public-like activity patterns.

Camera Coverage Context (Privacy-Relevant Framing)

s.15

s.15 There is no monitoring of private or sensitive spaces (e.g., washrooms or enclosed personal areas), and coverage is aligned with safety, security, and event coordination objectives.

A3.2 - Zone-Specific Camera Deployment Overview

CCTV is deployed to support crowd safety, ingress and egress management, and emergency response. Monitoring practices are designed to avoid unnecessary focus on individuals and remain proportionate to the operational context. Clear signage and public communication are used to inform attendees of CCTV use. These measures ensure that while the scale of monitoring is significant, it remains non-intrusive at the individual level and aligned with public safety objectives.

Zone 4: Event Approach near BC Place

This zone covers the final mile radius around BC Place in the downtown core of Vancouver. This includes three Skytrain stations: Yaletown-Roundhouse, Stadium-Chinatown, and Main Street-Science World.

A4.1 Zone Characteristics

A4.1.1 Density of Individuals
The zone experiences variable to high density, with significant surges during peak ingress and egress periods associated with event start and end times. Density is distributed along the corridor but may concentrate at transit stops, intersections, and entry screening points, where queuing and crowding can occur.

A4.1.2 Predictability of Movement
Movement within the zone is generally directional but not fully predictable. While most individuals are moving toward or away from the event venue, the corridor also accommodates public use, including pedestrians, commuters, cyclists, and vehicles not associated with the event. This results in a mixed-use flow with overlapping movement patterns, particularly at transit hubs and crossings.

A4.1.3 Presence of Vulnerable Populations
The zone includes a broad and unfiltered segment of the public, including children, elderly individuals, persons with disabilities, and other vulnerable populations. As a public thoroughfare, individuals may be present independently of the event, increasing the likelihood of incidental collection involving individuals who are not event attendees.

A4.1.4 Duration of Individual Presence
Individuals are present for short and transient durations, typically limited to the time required to pass through the corridor (e.g., walking, waiting for transit, or queueing). However, dwell times may increase temporarily at transit stops, intersections, or security screening areas during peak periods.

A4.1.5 Public vs. Semi-Public vs. Controlled Environment
This zone is a fully public environment, consisting of public streets and transit infrastructure. It is not access-controlled, and individuals may enter, exit, or remain within the space without restriction, regardless of their connection to the event. While it functions as an approach to a controlled/ticketed zone, it always retains its public character.

A4.1.6 Camera Coverage Context
s. 15 . s. 15 Given the public setting, cameras may incidentally capture a wide range of individuals, including non-event participants. There is no monitoring of private spaces, and coverage is limited to what is observable within the public realm, aligned with safety, security, and crowd management purposes.

A4.1.7 Zone-specific risk

This zone presents a distinct privacy profile characterized by high variability, full public exposure, and incidental collection of non-participants. The risk mitigations for this zone are grounded in the overt, non-intrusive nature of camera placement and the inherently public context of the environment.

A4.2 - Zone-Specific Camera Deployment Overview

CCTV is for aggregate movement and crowd flow monitoring rather than individual tracking. Video analytics, where used, are configured to support situational awareness and operational decision-making without profiling individuals. Monitoring is guided by predefined operational triggers, such as congestion or safety concerns, and does not involve persistent tracking of individuals across locations. This approach ensures that CCTV use remains proportionate and focused on maintaining safe and efficient movement within the zone.

Zone 5: Entertainment

This zone covers Commercial Drive between William St. and 1st Ave., as well as Granville Street between Davie St. and W Georgia St. This zone represents a higher privacy sensitivity context due to the combination of fully public exposure, diverse and potentially vulnerable populations, extended dwell times, and the presence of expressive activities such as protests. This is mitigated by the overt, non-intrusive, and non-targeted nature of camera coverage.

A5.1 Zone Characteristics Relevant to Privacy

A5.1.1 Density of Individuals

The zone experiences moderate to high density, with periodic peaks associated with transit flows, nightlife activity, and organized or spontaneous gatherings (e.g., community events or protests). Density varies by time of day, with elevated concentrations during evenings and major events.

A5.1.2 Predictability of Movement

Movement within the zone is highly variable and context dependent. While some directional flow is associated with transit use, the area also supports social, recreational, and expressive activities, including congregation and dispersal. Demonstrations or protests may result in non-linear and rapidly evolving movement patterns.

A5.1.3 Presence of Vulnerable Populations

The zone includes a broad and diverse cross-section of the public, including youth, individuals under the influence of alcohol or substances, persons experiencing homelessness, and individuals engaged in expressive activities. These contexts may involve individuals in heightened or sensitive circumstances, requiring careful consideration of proportionality and necessity in any monitoring approach.

A5.1.4 Duration of Individual Presence

Individuals may be present for both short and extended durations, reflecting the mixed-use nature of the area. While some individuals are transiting through, others may remain for prolonged periods for social, commercial, or expressive purposes, resulting in potential for repeated or sustained observation within a public setting.

A5.1.5 Public vs. Semi-Public vs. Controlled Environment

This zone is a fully public environment, consisting of public streets, sidewalks, and transit-adjacent spaces. It is open and accessible without restriction, and supports a wide range of lawful activities, including freedom of expression and peaceful assembly.

A5.1.6 Camera Coverage Context

s. 15 [redacted] The cameras do not track or single out individuals and are not deployed for the purpose of identifying participants in lawful activities such as protests or gatherings.

A5.1.7 Zone-specific risk
Given the nature of the environment, cameras may incidentally capture individuals engaged in expressive activities or other sensitive contexts. The design and operation of the system therefore emphasize minimization, proportionality, and avoidance of unnecessary intrusion, including limiting collection to what is visible within the public realm and avoiding the monitoring of private or interior spaces.

A5.2 - Zone-Specific Camera Deployment Overview

Camera placement and orientation are designed to prioritize sidewalks, roadways, and public gathering areas, with technical controls such as privacy masking and field-of-view restrictions applied to limit visibility into private spaces. Monitoring practices are governed by event-triggered protocols, ensuring that observation remains passive unless a defined safety or security concern arises. Public notification measures, including signage, are also implemented to enhance transparency and reduce the likelihood of unexpected observational concerns.

Zone 6: Hotel

This zone covers the exterior of official hotels, Jack Poole Plaza, and Vancouver Convention Centre.

A6.1 Zone Characteristics

A6.1.1 Density of Individuals
The zone experiences moderate to high density, with fluctuations based on hotel occupancy, convention schedules, and event timing. Peak periods may include check-in/check-out times, conference sessions, and event ingress/egress, resulting in concentrated activity at entrances, drop-off areas, and adjacent sidewalks.

A6.1.2 Predictability of Movement
Movement within the zone is generally structured but variable. Individuals primarily move between entrances, drop-off zones, parking areas, and nearby pedestrian routes. However, variability increases during conferences or large events, with congregation, queueing, and informal gathering occurring in exterior spaces.

A6.1.3 Presence of Vulnerable Populations
The zone includes a diverse population, including hotel guests, business travelers, event attendees, staff, and members of the public. While not inherently high-risk, individuals may be present in transient or situationally vulnerable states (e.g., fatigue, unfamiliarity with surroundings, carrying luggage, attending large events), and may include youth depending on event type.

A6.1.4 Duration of Individual Presence
Individuals are present for short to moderate durations. Many individuals pass through the space briefly (e.g., arrivals/departures), while others may remain for extended but bounded periods (e.g., waiting for transportation, socializing outside the venue, or transitioning between sessions).

A6.1.5 Public vs. Semi-Public vs. Controlled Environment

This zone is best characterized as a semi-public, mixed-use environment:

- *Public-facing exterior spaces* (e.g., sidewalks, drop-off areas) that are openly accessible, and
- *Access-mediated environments* (e.g., hotel and convention centre entry points) where access is functionally controlled but not strictly restricted.

As such, the area operates at the intersection of public thoroughfare and privately managed space.

A6.1.6 Camera Coverage Context

s. 15 s. 15 There is no monitoring of interior private spaces (e.g., guest rooms), and coverage is limited to areas where individuals would reasonably expect visibility in a public or semi-public context.

A6.1.7 Zone-specific risk

The Hotel Zone presents a distinct privacy risk profile due to the contextual sensitivity of access points and the nature of activities occurring within these environments. While camera deployment is limited to exterior areas, coverage of entrances and drop-off locations may enable inference of associations, relationships, or participation in specific events or meetings, particularly where individuals are observed entering or exiting at identifiable times.

This environment is also characterized by a heightened expectation of discretion, as individuals may reasonably expect a degree of anonymity in their movements despite being in publicly accessible spaces. The presence of business travellers, conference attendees, and potentially high-profile individuals further increases the sensitivity of incidental collection, including risks related to commercial confidentiality, reputational harm, or misinterpretation of observed activity.

While camera deployment at hotel entrances is more spatially focused than broader public-area coverage, it does not involve the identification or tracking of specific individuals. The purpose of deployment is to support general situational awareness and coordination at key access points, rather than to monitor or profile particular persons.

The Common Program does not use these cameras to identify individuals, track movements over time, or associate individuals with specific events or locations beyond what is incidentally observable in a public context. Additional safeguards, including restricted access, limited retention, and prohibition on targeted monitoring, are in place to mitigate the increased sensitivity associated with entrance-based observation.

A6.2 Zone-Specific Camera Deployment Overview

CCTV coverage for exterior, public-facing areas such as entrances, perimeters, and adjacent public spaces. Cameras are not oriented toward interior hotel environments or private guest areas. Monitoring remains event-driven and proportionate, with any focused observation

required to be justified, time-bound, and directly linked to an operational need. These controls ensure that the use of CCTV supports safety objectives while maintaining appropriate boundaries around personal privacy.

Annex B: Detailed Data Flow Diagrams

End-to-End Solution Architecture

s.15

Video Management System

s.15

Annex C: AI Model and Analytics Register

The Program maintains a centralized AI Model and Analytics Register that governs all analytical and decision-support capabilities enabled within the Camera System. The Register defines the purpose, inputs, outputs, permitted uses, and restrictions associated with each capability, along with the technical, administrative, and governance controls that apply. Only capabilities formally approved and recorded in the Register may be deployed, and all others are prohibited. Each entry is subject to defined accountability and human oversight requirements. This approach ensures that analytical functionality remains proportionate, transparent, and directly tied to the Program's operational objectives, while preventing unauthorized expansion or misuse.

A1 – Motion Detection (Baseline Triggering)

- **Category:** Detection
- **Operational Purpose:** Identify movement within defined camera zones to support situational awareness and operator attention
- **Program Alignment:** All zones (public safety and operational awareness)

Permitted Uses
- Trigger operator alerts for unusual or unexpected motion
- Support real-time monitoring

Explicitly Prohibited Uses
- Tracking individuals across cameras
- Inferring behaviour or intent

Data Inputs
- Live video feed (no storage required for processing)
- No external datasets

Processing Description
Detects pixel-level changes across frames to identify motion events; no identity or object classification involved

Outputs
- Visual alert flag
- No identification of individuals
- **Human review required**: Yes (always)

Risk Classification
- **Level:** Low
- **Key Risks:** Over-alerting, indirect behavioural inference

Controls & Safeguards
- No identity persistence
- Alerts not retained as behavioural profiles
- Access limited to authorized operators

Accountability

- **Owner:** City Operations Lead
- **Supervisor:** Program Director

A2 – Object Classification

- **Category:** Classification
- **Operational Purpose:** Identify general object types (e.g., vehicles,) to support operational awareness
- **Program Alignment:** Transportation and high-density zones

Permitted Uses
- Identify objects (e.g., “vehicle,”)
- Support incident detection

Explicitly Prohibited Uses
- Facial recognition
- Identification of individuals
- Demographic inference

Data Inputs
- Live and recorded video
- No external datasets

Processing Description
Applies trained models to classify objects into predefined, non-identifying categories

Outputs
- Object labels (e.g., “vehicle”)
- Alert flags
- **Human review required:** Yes

Risk Classification
- **Level:** Moderate
- **Key Risks:** Misclassification, inference creep

Controls & Safeguards
- Limited classification taxonomy
- No identity-linked outputs
- Periodic validation

Accountability
- **Owner:** Technical Systems Lead
- **Supervisor:** Privacy Office

A3 – Crowd Density Estimation (Aggregated Analytics)

- **Category:** Aggregation
- **Operational Purpose:** Assess crowd levels for safety and operational planning

- **Program Alignment:** Event zones, high-traffic areas

Permitted Uses
- Generate crowd density metrics
- Inform operational decisions (e.g., resource allocation)

Explicitly Prohibited Uses
- Individual tracking
- Identifying specific persons within crowds

Data Inputs
- Video feeds (processed into anonymized counts)

Processing Description
Estimates number of individuals in a frame using aggregation techniques without identifying individuals

Outputs
- Numeric density metrics
- Heat maps
- **Human review required:** Yes

Risk Classification
- **Level:** Moderate
- **Key Risks:** Re-identification in low-density scenarios

Controls & Safeguards
- Minimum aggregation thresholds
- Suppression in low-count environments
- No individual-level outputs

Accountability
- **Owner:** Analytics Lead
- **Supervisor:** Program Director

A5 – Incident Alerting / Rule-Based Analytics

- **Category:** Detection / Decision-Support
- **Operational Purpose:** Trigger alerts based on predefined rules (e.g., restricted area entry)
- **Program Alignment:** All zones

Permitted Uses
- Alert on predefined operational conditions
- Support operator awareness

Explicitly Prohibited Uses
- Autonomous decision-making
- Enforcement actions without human review

Data Inputs
- Video feeds
- Configured rules

Processing Description
Applies rule-based logic (not adaptive AI) to detect predefined conditions

Outputs
- Alerts
- Event logs
- **Human review required:** Yes

Risk Classification
- **Level:** Low
- **Key Risks:** Over-reliance, alert fatigue

Controls & Safeguards
- Rule validation
- Operator confirmation required

Accountability
- **Owner:** Operations Manager
- **Supervisor:** Program Director

A6 – Aggregated Reporting & Trend Analysis

- **Category:** Aggregation / Analytics
- **Operational Purpose:** Generate post-event insights and operational reports
- **Program Alignment:** Program-level evaluation

Permitted Uses
- Trend reporting
- Operational performance analysis

Explicitly Prohibited Uses
- Individual profiling
- Cross-dataset identity linkage

Data Inputs
- Aggregated system data
- Event logs

Processing Description
Analyzes aggregated, non-identifiable data to identify patterns and trends

Outputs
- Reports
- Dashboards

- **Human review required:** Yes

Risk Classification
- **Level:** Low–Moderate
- **Key Risks:** Re-identification through small datasets

Controls & Safeguards
- Aggregation thresholds
- Data suppression rules
- No raw footage in reports

Accountability
- **Owner:** Analytics Lead
- **Supervisor:** Privacy Office

A7 – PROHIBITED: Facial Recognition

- **Category:** Prohibited Capability
- **Operational Purpose:** Not permitted

Explicit Prohibition
The following capabilities are **strictly prohibited**:
- Facial recognition
- Emotion detection
- Demographic inference (e.g., age, gender, ethnicity)

Rationale
- Not necessary for program purpose
- Disproportionate privacy intrusion
- Elevated regulatory and reputational risk

Controls
- Technical disablement of features
- Contractual prohibitions with vendors
- Periodic verification and audit

Risk Classification
- **Level:** High (if enabled)

Accountability
- **Owner:** Program Governance Committee
- **Supervisor:** Privacy Office

Annex D: Privacy Risk Register

Risk #	Risk	Description	Likelihood	Impact	Risk Score	Mitigation Measure	Mitigated Likelihood	Mitigated Impact	Residual Risk Score
R1	Unclear Governance Roles	Ambiguity between governance partners and operational participants leads to inconsistent decision-making and accountability gaps	s.13(1)			Formal governance framework; clearly defined roles in agreements; decision-rights matrix	s.13(1)		
R2	Unauthorized Data Access	Improper access to camera footage or analytics data by partners or personnel				Role-based access controls, audit logs, least privilege enforcement			
R3	Function Creep	Data collected for event security used for unrelated purposes				Purpose limitation clauses; contractual restrictions; audit oversight			
R4	Multi-Partner Misalignment	Inconsistent practices across up to participant partners creating compliance gaps				Common program agreement; standardized policies; onboarding requirements			

R5	AI Alert Misinterpretation / Over-Reliance	Users may place undue reliance on AI-generated or AI-prioritized alerts without sufficient validation of context, underlying data, or operational relevance. This may result in inappropriate prioritization, delayed response to more critical issues, or unnecessary action based on alerts that are incomplete, outdated, or not operationally significant.	s.13(1)	Human review required before actioning alerts Training on alert limitations, thresholds, and appropriate use Clear documentation of alert logic and intended use Operational procedures requiring validation against current conditions	s.13(1)
R6	Time-Limited Program Drift	Temporary program evolves into longer-term use without reassessment		Explicit sunset clauses; decommissioning plan; enforced end-date controls	
R7	Algorithmic Bias	AI analytics produce biased or unfair outcomes affecting individuals/groups		Pre-deployment testing; bias monitoring; restricted use cases	
R8	Security Breach	External or internal breach exposing sensitive surveillance or personal data		Encryption, monitoring, incident response plan, penetration testing	
R9	Regulatory Non-Compliance	Failure to meet FIPPA or regulator expectations		Ongoing regulator engagement; PIA alignment; legal review	
R10	Reputational Damage	Public/media concern due to perceived surveillance overreach		Transparency strategy; stakeholder engagement; clear messaging	

			s.13(1)		s.13(1)
R11	Third-Party Vendor Risk	Vendors mishandle data or fail to meet contractual/privacy obligations		Strong contractual terms; vendor assessments; monitoring	
R12	Incidental Capture of Sensitive Activities	Cameras capture individuals in sensitive but lawful contexts (e.g., protests, nightlife behaviour, medical distress)		Non-targeted camera design; avoid zoom/targeting; strict use limitations; retention minimization	
R13	Perceived Surveillance of Charter-Protected Activities	Public perception that cameras are used to monitor protests or assemblies		Explicit policy prohibitions; Charter-aware framing; public communications; oversight	
R14	Secondary Use Pressure from External Agencies	External entities request access to footage due to public/high-interest locations		Strict disclosure protocols; legal thresholds; documentation and oversight	
R15	Insufficient Demonstration of Necessity	Deployment challenged as not necessary or proportionate to objectives		Documented rationale per zone; regulator alignment; proportionality analysis	
R16	Data Retention Overreach	Data retained longer than necessary or inconsistently across partners		Program-level retention standards; automated deletion	
R17	Inadequate Training	Staff or partners misunderstand obligations or system use		Mandatory training; role-specific guidance	

			s.13(1)		s.13(1)
R18	Video Monitoring of Non-Event Populations	Non-participants (commuters, residents, passersby) are incidentally captured by cameras		Clear purpose limitation; geographic justification; signage beyond event perimeter	
R19	Inconsistent Notice in Fluid Environments	Individuals enter monitored areas without encountering signage		Distributed signage strategy; placement at transit hubs and key flow points	
R20	Misapplication of "Public Space" Assumptions	Public environments treated as lower risk than appropriate		Context-sensitive design; Charter-aware analysis	
R21	Perception of Targeted VIP Monitoring	Use of cameras at hotel entrances for VIP coordination creates perception that specific individuals are being monitored or tracked		Clear policy prohibiting targeted monitoring; operational protocols limiting use to situational awareness; training and oversight	
R22	De Facto Individual Tracking Through Repeated Observation	Repeated viewing of the same entrance points enables informal tracking of individuals over time without technical tracking tools		Limit retention; restrict continuous monitoring; reinforce prohibition on tracking; audit access patterns	
R23	Inference of Event or Hotel-Specific Attendance	Observation of individuals entering specific hotels allows inference of attendance at particular events, meetings, or affiliations		Non-targeted use; limit access to footage; prohibit use for attendance or affiliation analysis; retention limits	

			s.13(1)		s.13(1)
R24	Elevated Sensitivity Due to Purpose (VIP Coordination)	Explicit linkage of camera deployment to VIP coordination increases scrutiny and sensitivity of observed activities		Clearly define purpose as situational coordination, not individual monitoring; governance controls; documentation of use limitations	
R25	Operational Drift Toward Individual-Level Awareness	Operators may shift from situational awareness to focusing on specific individuals due to operational pressures or expectations		Training; supervision; clear use protocols; audit logs; enforcement of prohibited uses	
R26	Inadequate Collection Notice	Failure to meet legal requirements for meaningful notice		Standardized signage + zone-specific adaptations; legal review of wording	
R27	Improper Disposal	Failure to securely dispose of data at end of lifecycle or program		Secure deletion protocols; disposal verification; audit trails	
R28	Data Accuracy Issues	Inaccurate or incomplete data leading to incorrect decisions or outputs		Data validation processes; system checks	
R29	Complaint Handling Failures	Inadequate response to public complaints or access requests		Formal complaint process; tracking; escalation pathways	
R30	Partner Exit Risk	Improper data handling when a partner leaves the program		Exit procedures; access revocation; data return/destruction requirements	

R31	Over-Collection of Data	Collection of more data than necessary for stated purpose	s.13(1)				Data minimization controls; camera positioning review; configuration standards	s.13(1)		
R32	Lack of Auditability	Inability to demonstrate compliance due to poor logging or documentation					Comprehensive logging; periodic audits; reporting dashboards			
R33	Scope Misinterpretation	Public or stakeholders misunderstand what is actually being monitored					Clear signage, FAQs, and communications clarifying scope and limitations			
R34	Disproportionate Impact on Specific Communities	Video monitoring disproportionately affects certain groups due to geographic placement					Equity impact consideration; non-targeted deployment; policy restrictions			
R35	Misinterpretation of Behaviour in Dynamic Environments	Observational footage is misinterpreted leading to incorrect responses					Operator training; contextual guidance			
R36	Crowd-Induced Loss of Context	High-density reduces ability to interpret individual actions					Use footage for situational awareness only; reinforce limitations			
R37	Video Monitoring Spillover Beyond Intended Zone	Camera fields of view extend into unintended areas					Camera positioning audits; masking/privacy zones			
R38	Unequal Visibility of Monitoring	Certain areas appear more heavily monitored than others					Balanced deployment rationale; documented site selection criteria			
R39	Perceived Monitoring of Guest Movements	Hotel guests perceive monitoring of arrivals/departures					Clear signage; limit camera focus; avoid tracking			

R40	Commercial / Reputational Sensitivity for Venue Operators	Perception impacts hotel or convention centre relationships	s.13(1)	Coordinated communications; consistent messaging	s.13(1)
R41	Overlap with Existing Private Camera Systems	Confusion between program and venue-operated systems		Clear delineation of systems; their intended purpose; no integration	
R42	Queue and Congregation Visibility Risk	Entrances create concentrated capture and pattern visibility		Limit retention; no pattern analysis	
R43	Blurred Public–Private Boundary	Individuals unclear about authority or monitoring context		Clear signage; public documentation of authority	
R44	Limited Ability to Support Access Requests	Difficulty locating footage for access requests		Defined procedures; search protocols; expectations management	
R45	Inconsistent Application of Privacy Controls Across Zones	Variation in controls across zones creates uneven protection		Standardized configurations; audits; oversight	
R46	Misinterpretation of Presence at Specific Hotel	Observation of an individual at a hotel entrance may lead to incorrect assumptions about their purpose, affiliation, or activities		Restrict interpretive use; reinforce situational-only purpose; training on limitations of observation	
R47	Concentration of Video Monitoring at High-Sensitivity Locations	Focusing cameras on hotel entrances concentrates monitoring in areas with inherently higher contextual sensitivity		Justify placement through necessity analysis; limit number of cameras; periodic review of deployment	

R48	Implicit Expectation of Monitoring by Stakeholders	Stakeholders may assume cameras are being used to actively monitor or track VIPs, creating pressure to expand use beyond intended scope	s.13(1)	Clear communication of system limitations; governance controls; reinforce non-targeted use in operational protocols	s.13(1)
R49	Environmental Factors Affecting Data Quality	Lighting, weather, and density degrade footage quality		Acknowledge limitations; restrict use cases; training	
R50	Unauthorized Physical Access to Monitoring Stations	Individuals gain physical access to monitoring environments		Controlled facilities, restricted zones, badge access	
R51	Unauthorized Export of Video Data	Improper extraction or disclosure of footage		Export controls, approvals, logging	
R52	Non-Operational Use of Footage by Authorized Staff	Authorized users access footage for inappropriate purposes		Policies, RBAC, audit logs, enforcement	
R53	Delayed Detection of Misuse	Misuse of access is not identified in a timely manner		Monitoring, alerting, audit reviews	
R54	Credential Compromise (Phishing/Social Engineering)	User credentials compromised leading to unauthorized access		Training, monitoring, limited access to terminals, disconnection of overall system from the world-wide internet	
R55	Capture of Sensitive Affiliations or Events	Individuals attending sensitive events are incidentally captured		Non-targeted use; restrict identification; minimize retention	
R56	Targeted Attention to High-Profile Individuals	VIPs or dignitaries create heightened sensitivity		Prohibit targeted monitoring; strict controls	

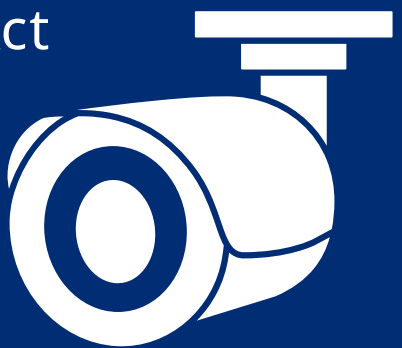
R57	Event-Specific Sensitivity Amplification	Certain events increase contextual sensitivity	s.13(1)	Context-aware deployment review; reinforce purpose limitation	s.13(1)
R58	Re-Identification Through Data Linkage	Data combined with other datasets to identify individuals		Prohibit linkage; restrict analytics outputs; governance controls	
R59	Informal or Unauthorized Disclosure Outside Processes	Staff share information or footage outside approved channels		Training; policy enforcement; monitoring	
R60	Telecomm Outage / Disruption	Loss of connectivity impacts availability of feeds		Monitoring, alerting, fallback procedures	
R61	Residual Perception Risk Despite Safeguards	Public concern persists despite mitigations		Transparency; communications; stakeholder engagement	
R62	Unauthorized Physical Access to Data Centre Infrastructure	Physical compromise of infrastructure hosting data		Secured facilities; access controls; audits	
R63	Insider Threat Despite Controls	Malicious or negligent insider misuse		Logging; oversight; anomaly detection	
R64	Lack of Traceability for Footage Access	Inability to link access to a specific user		Comprehensive logging; immutable audit trails	
R65	Unauthorized Use of Analytics Capabilities	Use of prohibited analytics (e.g., facial recognition)		Technical restrictions; contractual prohibitions; audits	

Annex E: Collection Notices and Transparency Materials

9x9 in

This area is temporarily monitored by CCTV during a special event period.

By entering this zone, your personal information is collected under section 26(c) of the Freedom of Information and Protection of Privacy Act for the purpose of providing situational awareness and ensuring safety and security during the special event period.



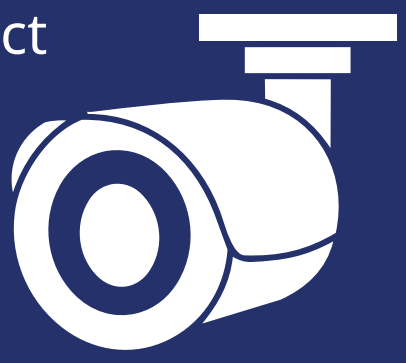
Your privacy is important to us.

If you have any questions, please contact: privacy@vancouver.ca

CITY OF VANCOUVER

This area is temporarily monitored by CCTV during a special event period: June 7 to July 19, 2026

By entering this zone, your personal information is collected under section 26(c) of the Freedom of Information and Protection of Privacy Act for the purpose of providing situational awareness and ensuring safety and security during the special event period.



Your privacy is important to us.

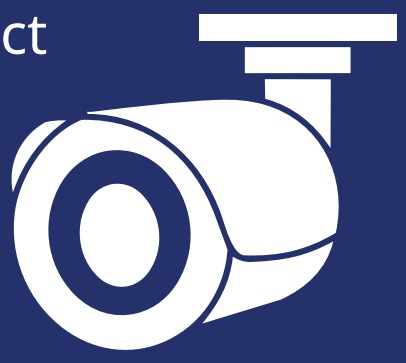
If you have any questions, please contact: privacy@vancouver.ca

CITY OF VANCOUVER

BC PLACE VANCOUVER AREA

This area is temporarily monitored by CCTV during a special event period: June 7 to July 19, 2026

By entering this zone, your personal information is collected under section 26(c) of the Freedom of Information and Protection of Privacy Act for the purpose of providing situational awareness and ensuring safety and security during the special event period.



Your privacy is important to us.

If you have any questions, please contact: privacy@vancouver.ca

CITY OF VANCOUVER

Appendix A: Definitions

Analytics Metadata: Structured data generated by video analytics software that describes events or objects detected within video footage (e.g., time, location, object classification, movement path, or event trigger). Analytics metadata does not constitute standalone evidence and is used primarily to assist operators in locating relevant video segments.

Audit Log: A system-generated record documenting user activity within the video management or analytics platform, including access to video footage, search queries, exports, configuration changes, and other administrative actions.

Authorized User: An individual who has been granted system credentials and role-based permissions to access the camera system for approved operational purposes in accordance with program governance policies.

Camera System: The integrated combination of cameras, network infrastructure, video management software, analytics software, and storage systems used to collect, process, and retain video footage specific to the Common Program.

Common Program: The program described in section 1 of the PIA and signed onto by its Governance and Operational partners.

Emergency Operations Centre (EOC): The City of Vancouver's centralized physical facility established to coordinate information, resources, and decision making among authorized organizations during emergencies or significant incidents.

Event Alert means a notification generated by the video analytics component of the Camera System when a predefined operational rule or condition is met. An Event Alert may include a still image or a brief video clip derived from camera footage for the limited purpose of enabling authorized personnel to quickly assess the relevance of the detected event. Event Alerts do not constitute a system of record, do not replace or duplicate video footage stored within the Video Management System (VMS), and are not retained independently of the underlying footage.

Governance Partners: Defined in the Common Program Agreement, the City and VPD, and, if applicable, any other public body brought into the class of Governance Partner via the mechanisms in the Common Program Agreement. These partners participate in the program and share governance responsibilities for the system, including policy oversight, operational coordination, and compliance with applicable privacy and legal requirements.

Object Detection: A video analytics capability that identifies and categorizes objects appearing in video footage (for example, pedestrians, vehicles, or bicycles) using algorithmic analysis.

On-Premises Data Storage: A storage architecture in which video footage and associated system data are stored within a physical data centre or server environment controlled by program partners rather than in external cloud infrastructure.

Operational Partners: Organizations that may receive operational benefits from the camera program (such as situational awareness or coordination support) but do not participate in governance or decision-making regarding system operation.

Participant Organizations: Organizations involved in the camera program that are designated as either Governance Partners or Operational Partners, as defined in this document.

Role-Based Access Control (RBAC): A security mechanism that restricts system access based on the authorized role of the user. Permissions are assigned according to operational responsibilities, ensuring that users can access only the information necessary to perform their duties.

Searchable Video Analytics: A functionality that allows operators to identify segments of video footage based on characteristics such as object type, movement patterns, time range, or defined zones within the camera field of view.

Situational Awareness Monitoring: The real-time or near-real-time observation of camera feeds to support public safety coordination, operational response, or event management activities.

Video Analytics: Automated software processes that analyze video footage to detect objects, movement patterns, or predefined conditions.

Video Export: The controlled process of extracting video footage from the system for authorized investigative, evidentiary, or operational purposes.

Video Management System (VMS): Software used to manage camera feeds, control recording functions, store video footage, and facilitate authorized retrieval or playback of recorded footage. In this case, it refers to the product s.15

Video Redaction: The process of obscuring identifiable elements within video footage (such as faces, license plates, or other personal identifiers) before disclosure.

Viewing Station: A secured workstation or physical location from which authorized users can access live or recorded video footage within the system.

VPD Ops Centre: A centralized physical facility established by the VPD to coordinate command and control.

Appendix B: Common Program Agreement

FWC26 COMMON PROGRAM AGREEMENT (the "Agreement")

THIS AGREEMENT is between:

City of Vancouver, 453 West 12th Avenue, Vancouver, British Columbia, V5Y 1V4,
Attn: Sandra Singh (Deputy City Manager) (the "**City"**)

AND

Vancouver Police Department, 2120 Cambie Street, Vancouver BC V5Z 4N6
Attn: Chief Constable Steve Rai ("the **VPD**")

BACKGROUND:

A. The Vancouver Police Department is a municipal police department and public body, constituted in accordance with the BC *Police Act* and possesses the authority to conduct law enforcement investigations, preserve the peace, prevent crime and offences and protect the public.

B. The City is a municipality responsible for the delivery of municipal services and the safety and security of persons within the City of Vancouver.

C. The City and VPD are jointly responsible for the delivery of a common program of public safety and security in connection with the FIFA World Cup 2026 ("**FWC26**"), to be hosted in Vancouver, British Columbia (the "Common Program").

D. The Common Program involves the collection, use, and disclosure of personal information, and the parties wish to confirm the Common Program as a common or integrated program or activity within the meaning of Schedule 1 of the Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165 ("**FIPPA**") and the Freedom of Information and Protection of Privacy Regulation, B.C. Reg. 155/2012 (the "**FOIPP Regulation**").

E. This Agreement is intended to constitute a common or integrated program agreement for the purposes of section 12 of the FOIPP Regulation, confirming the Common Program as a common or integrated program or activity under FIPPA.

F. Certain public bodies and other agencies will participate in the Common Program as operating participants (each, an "**Operational Participant**" and collectively, the "**Operational Participants**") and will be bound by the terms of this Agreement through the execution of an Access and Information Sharing Agreement in the form approved by the parties. This Agreement, together which each executed Access and Information Sharing Agreement, is intended to constitute the written documentation confirming the Common Program as common program or activity for the purposes of section 12 of the FOIPPA Regulation.

1. Program Purpose and Scope

1.1. Program Purpose

The purpose of the Common Program is to support the safety, security, situational awareness, incident response and operational coordination of FWC26 through lawful collection, use, and disclosure of personal information and related operational data (collectively, the "**Program Data**") by the Governance Participants and Operational Participants, in accordance with FIPPA and this Agreement (the "**Program Purpose**"). The Common Program provides coordinated real-time situational awareness during FWC26 through a shared temporary camera network and video management capability, under the governance, control, and direction of the Governance Participants.

1.2. **Governance Structure**

The City and the VPD jointly govern and operate the Common Program as governance partners (each, a "**Governance Participant**"). Each Governance Participant acts as a primary custodian of Program Data within its respective sphere of authority and is responsible for ensuring that the collection, use, and disclosure of Program Data by Operational Participants is authorized, proportionate, and consistent with the Program Purpose. Personal information may be disclosed to Operational Participants only to the extent necessary for the operation of the Common Program within their respective spheres of operational responsibility.

1.3. **Camera Network**

The Common Program is built on a hub and spoke model and operates a network of approximately 200 cameras deployed across six zones in the City of Vancouver (the "**Camera Network**"), which includes: (a) Killarney Training Facility; (b) UBC National Soccer Training Centre; (c) FanFest (PNE); (d) Event Approach (Last Mile radius) near BC Place;(e) Entertainment Zone; and (f) Hotel Zone.

1.4. **Program Data**

The data collected, used, and disclosed from the Common Program include live video streams, analytic alerts, still image captured, system-generated metadata, attribute descriptors (eg direction of travel), and aggregated statistical outputs (eg population count). Directly identifiable information will include direct visual identifiers, temporal location data, quasi-identifiers (eg. Approximate age), and inferred data (eg. object and behavioural inferences, activities such as loitering and queuing, and crowd formation. (collectively, the "**Program Data**"). For greater certainty, behavioural inferences are made solely through human observation and not through automated video analytics.

2. Collection, Use and Disclosure

2.1. The Governance Participants collect Program Data under sections 26(b) and 26(c) of FIPPA. All Operational Participants collect Program Data under sections 26(a) and 26(c) of FIPPA.

2.2. Operational Participants that rely on section 26(a) of FIPPA as their collection authority acknowledges that they are responsible for ensuring that such authority exists under their applicable enabling legislation. Where no other collection authority applies, section 26(c) of FIPPA is the primary collection authority for all CPA Participants.

2.3. Program Data is used and disclosed by all CPA Participants under sections 32 and 33 of FIPPA, including 32(c) and 33(2)(k), as applicable..

2.4. The public will be notified of the collection of personal information through signage posted around the perimeter of all monitored areas, positioned so as to be visible to individuals prior to entering the range of the Camera Network.

3. Governance Council

3.1. The Governance Council shall consist exclusively of designated representatives of the Governance Participants. (the "**Governance Council**").

3.2. Each Governance Participant may admit additional Operational Participants as they require to ensure the objectives of the Common Program and shall provide notice to the other of the included Operational Participants.

3.3. Any admission of an additional Governance Participant shall require the unanimous written agreement of the existing Governance Participants.

4. Classes of Participants

4.1. Governance Participants (Class A)

Governance Participants are responsible for determining the purpose, scope, parameters, retention standards, technology approvals, and policy framework of the Common Program, which includes:

(a) approving and amending the Program Purpose;
(b) determining categories of data collected;
(c) approving technology and vendor procurement;
(d) approving and overseeing camera locations, installation, angles;
(e) approving and overseeing Privacy Impact Assessments (PIAs);
(f) determining the manners in which personal information is disclosed to Class B Operational Participants;
(g) establishing retention and destruction schedules;
(h) admitting or removing Operational Participants;
(i) responding to freedom of information requests as the party with custody and control;
(j) correcting or annotating records in accordance with FIPPA sections 28 and 29.

4.2. Operational Participants (Class B)

Operational Participants may collect or access Program Data only within the scope authorized by the Governance Council. Operational Participants:

(a) shall not determine Program Purpose or scope;
(b) shall not expand data collection categories, except as authorized FIPPA and supported by their own enabling legislation;
(c) shall comply with this Agreement and any written operational policies, privacy and security instructions issued by the Governance Council for the Common Program; and
(d) give all reasonable assistance to the Governance Council in the event of an audit or investigation of collection, use, and disclosure practices related to Program Data.

4.3. **Permitted Uses (Operational Participations)** Operational Participants may use Program Data only for the Program Purpose and only to the extent necessary to carry out their operational responsibilities within the Common Program, including:

(a) observing Program Data in real time for situational awareness, incident response and operational coordination;

(b) communicating relevant situational information derived from Program Data to their Personnel and to other CPA Participants on a strict need-to-know basis for the Program Purpose; and

(c) where required for an authorized operational purpose, requesting access to, or retention of, specific video footage through the Governance Council, with the requestor's rationale and lawful authority.

4.4. **No Copying / No Retention / No Secondary Use**. Operational Participants shall not, and shall ensure their Personnel do not, copy, record, photograph, screenshot, download, extract, retain, or otherwise reproduce Program Data, except where the Governance Council has expressly authorized retention or disclosure in accordance with this Agreement and applicable law.

4.5. Operational Participants shall not use Program Data for any purpose unrelated to the Program Purpose or otherwise not expressly authorized under this Agreement and applicable law.

5. Access Requests

5.1. Operational Participants who receive an access request for records related to the Common Program must refer requests to the Governance Participants and advise the applicant that the records may be in the custody of the Governance Participants.

5.2. Operational Participants who receive an access request for Program Data within their own custody, including footage received under section 2 of this Agreement, must consult with the Governance Participants prior to making any disclosure.

5.3. Operational Participants receiving a request for correction or annotation must refer the request to the Governance Council.

6. Privacy and Legal Compliance

6.1. Each Governance Participant warrants that it has lawful authority under FIPPA or other applicable law to collect and authorize the collection of Personal Information under the Common Program.

6.2. The parties acknowledge that a Privacy Impact Assessment (PIA) is in progress and shall be finalized and approved by the Governance Council prior to the implementation of the Common Program.

7. Retention and Destruction

7.1. Video footage flowing through the video management system is captured for a 30-day period, after which it is overwritten or deleted.

7.2. Program Data may be retained by the Governance Participants when there is a legal or law enforcement reason to capture and store that data separately.

7.3. Information used to make a decision about identifiable individuals shall be retained for a minimum of one year.

8. Program Specific Security Controls

8.1. Each CPA Participant shall implement and maintain reasonable administrative, technical, and physical safeguards appropriate to the sensitivity of the Program Data in its custody or control and shall ensure that access to Program Data is limited to those of its Personnel who require access for the purposes of the Common Program.

8.2. Operational Participants may only access Program Data though direct observation via the Common Program. Operational Participants who require video footage must submit a request to the Governance Council with their rationale and legal authority for the request.

8.3. Only the Governance Participants may retain any footage, and only where authorized by law or for law enforcement purposes. Only designated Governance Participant staff shall have the technical capability to mark footage for retention beyond the standard 30-day period.

8.4. All access to Program Data is governed by role-based access control system, as implemented by the Governance Participants for the Common Program.

8.5. All footage is transmitted over a secure network that is not accessible via the internet and is stored on premises in a physically secured facility with restricted keycard access.

8.6. The Common Program incorporates technological controls that prohibit the use of facial recognition technology. Governance Participants and Operational Participants (collectively, the

CPA Participants") shall not apply facial recognition algorithms to any footage or Program Data disclosed for the Common Program as part of the Common Program, nor use Program Data for any purpose not authorized under this Agreement.

8.7. Each CPA Participant shall promptly notify the Governance Council upon becoming aware of any actual or suspected vulnerability in its systems that may affect the security or integrity of Program Data.

9. Liability and Indemnification

9.1. In this section, "**Personnel**" means, in respect of a party, its officers, employees, agents and contractors.

9.2. Each party is responsible for its own acts and omissions and those of its Personnel in connection with the Common Program.

9.3. Each Operational Participant shall indemnify and hold harmless each Governance Participant and its Personnel from and against any direct losses, claims, damages, costs, and expenses (including reasonable legal fees) arising out of or in connection with:

(a) any unauthorized use or disclosure of Program Data by that Operational Participant or its Personnel;
(b)
(c) any use of Program Data by that Operational Participant or its Personnel outside the Program Purpose;
(d)
(e) any attempt by that Operational Participant or its Personnel to access, download, extract, or retain Program Data beyond direct observation through the Common Program; or
(f)
(g) any failure by that Operational Participant to report a Program Data Incident in accordance with section 10 of this Agreement.

This indemnity does not extend to losses arising from a Governance Participant's own negligence or wilful misconduct.

10. Incident Management

10.1. In this section, "**Program Data Incident**" refers to any actual or suspected unauthorized collection, use, or disclosure of Personal Information in connection with the Common Program.

10.2. Any CPA Participant who becomes aware of a Program Data Incident shall report it to (a) the Director of Access to Information & Privacy at the City of Vancouver by telephone and email at privacy@vancouver.ca; and (b) the Governance Council, within 24 hours of discovery and shall reasonably cooperate with the Governance Council as it is required in connection with the investigation, containment, and remediation of the Program Data Incident.

10.3. The Governance Council shall investigate any Program Data Incident and determine whether the incident poses a real risk of significant harm to affected individuals, which may require notification to the affected individuals or the Office of the Information and Privacy Commissioner for British Columbia.

10.4. CPA Participants shall provide all reasonable assistance requested by the Governance Council in the investigation, containment, and remediation of a Program Data Incident.

11. Termination and End of Program Destruction

11.1. The Common Program is time-limited and will start on the effective date and conclude no later than July 21, 2026.

11.2. Upon termination, all CPA Participants shall securely destroy or return any Program Data as directed by the Governance Council, except where retention is required by law.

12. General

12.1. This Agreement is governed by and shall be construed in accordance with the laws of the Province of British Columbia.

12.2. This Agreement may only be amended by written agreement signed by both Governance Participants. No amendment shall be effective unless it is in writing and executed by both Governance Participants. The Governance Participants shall provide reasonable notice to all Operational Participants of any amendment that materially affects their rights or obligations under this Agreement.

12.3. Any notice required or permitted under this Agreement must be in writing and may be given by personal delivery, overnight courier, or mail to the address of the receiving Governance Participant. Notices shall be deemed to have been received:(a) on the date of delivery, if delivered by personal delivery; (b) on the next business day, if sent by overnight courier; or (c) on the third business day following the date of mailing, if sent by prepaid mail.

For greater certainty, email is not valid for notices required under this Agreement but may be used for operational communications.

12.4. The terms of this Agreement will form Schedule B of the EOC Access and Information Sharing Agreement between the City and each Operational Participant (the "**AISA**") and shall be read together with the AISA. In the event of a conflict between the terms of this Agreement and the AISA with respect to the collection, use, or disclosure of personal information, the CPA prevails.

Agreed to on behalf of the City of Vancouver

Sandra Singh Deputy City Manager	Date

Agreed to on behalf of the Vancouver Police Department

[NTD: to confirm] Chief Constable, Vancouver Police Department	Date