

File No.: 2026-457

August 7, 2026

s.22(1)

Dear s.22(1)

Re: **Request for Access to Records under the Freedom of Information and Protection of Privacy Act (the "Act")**

I am responding to your request of May 20, 2026 under the ***Freedom of Information and Protection of Privacy Act*** for:

Records related to the temporary CCTV surveillance network being deployed by the City of Vancouver and the Vancouver Police Department (VPD) in connection with the 2026 FIFA World Cup:

1. Any Privacy Impact Assessment (PIA) prepared by, or on behalf of, the City of Vancouver or the VPD relating to the FIFA World Cup 2026 CCTV program;
2. Any draft, interim, or final versions of the above PIA, including any revisions made following consultation with the Office of the Information and Privacy Commissioner of BC (OIPC);
3. The "Common Program Agreement" between the City of Vancouver and the VPD governing the operation of the FIFA World Cup 2026 CCTV network;
4. Any data-sharing agreements, protocols, memoranda of understanding, or other records governing the sharing of CCTV footage with FIFA, the FIFA World Cup 2026 Vancouver Host Committee, or any security contractors;
5. Any records describing the data retention schedule for footage collected by the FIFA World Cup 2026 CCTV network; and
6. Any records of communications between City staff and FIFA, or between City staff and the Vancouver Host Committee, regarding the storage, transfer, or use of CCTV footage outside of Canada.

Date range: January 1, 2024 to May 19, 2026.

Some of the responsive records are attached*. The records responsive to point two have been withheld in full under s.13(1) of the Act. You can read or download this section or these sections here: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00.

*Please note, the records responsive to point one are publicly available. You can find them on the City of Vancouver's website at the following link: <https://vancouver.ca/files/cov/city-of-vancouver-proactive-release-FWC26-situational-awareness-PIA.pdf>.

Additionally, regarding point six of your request, staff have advised our office that the City does not have any communications regarding the storage or use of CCTV footage outside of Canada as no CCTV footage will be stored, used, or transferred outside of Canada.

Under Part 5 of the Act, you may ask the Information & Privacy Commissioner to review any matter related to the City's response to your FOI request by writing to: Office of the Information & Privacy Commissioner, info@oipc.bc.ca or by phoning 250-387-5629.

If you request a review, please provide the Commissioner's office with: 1) the request number (2026-457); 2) a copy of this letter; 3) a copy of your original request; and 4) detailed reasons why you are seeking the review.

Yours truly,

Kevin Tuerlings, FOI Case Manager, for

[Signed by Kevin Tuerlings]

Siân Madsen, MA, MAS
Acting Director, Access to Information & Privacy

If you have any questions, please email us at foi@vancouver.ca and we will respond to you as soon as possible. You may also contact 3-1-1 (604-873-7000) if you require accommodation or do not have access to email.

Encl. (Response Package)

:kt

**EMERGENCY OPERATIONS CENTRE (EOC)
ACCESS AND INFORMATION SHARING AGREEMENT (the "Agreement")**

THIS AGREEMENT is between:

City of Vancouver, 453 West 12th Avenue, Vancouver, British Columbia, V5Y 1V4,
Attn: Legal Services, Francie J. Connell (City Solicitor and Director of Legal Services)
(the "**City**")

AND

[Full Legal Name of Participant Organization], [Street], [City, Province, Postal Code], Attn: [Contact Person];
(the "**Participant**")

This Agreement is effective as of [month], [date], 2026 (the "**Effective Date**")

BACKGROUND:

- A. The City is a host city for FIFA World Cup 2026 in Vancouver, British Columbia ("**FWC26**") and has, with partner organizations, established a command, control, coordination, and communication structure (the "**C4 Structure**") to coordinate planning and operational delivery of FWC26.
- B. To support that coordination the City operates a suite of digital tools, the C4 Information Management Solutions, that provide C4 Structure participants with a shared operational picture, situational awareness, and coordination capability during FWC26.
- C. The Participant is an agency or partner organization participating in or supporting the C4 Structure and requires access to some or all the C4 Information Management Solutions.
- D. The City is prepared to grant the Participant access to the C4 Information Management Solutions on the terms of this Agreement, which also governs how information shared through the tools are used, protected, and kept confidential.
- E. Where the Participant is identified as a CPA Participant in Appendix 2, it is also is subject to the Common Program Agreement (CPA) terms in Schedule B, which govern its access and use of the CPA Program Data (as defined in Schedule B) in connection with FWC26.

PARTICIPANT SPECIFIC DETAILS

C4 Information Management Solutions	[SharePoint, VanORCA, Unity Lense, Common Operating Platform (Limited)]
CPA Participant	[Yes/No]

The schedules to this Agreement are intended to govern distinct subject matters and form part of this Agreement. Schedule A governs access to and use of the City's C4 Information Management Solutions. Schedule B governs the collection, use, and disclosure of personal information in connection with the Common Program. In the event of a conflict or inconsistency between this Agreement and its schedules, the following order of precedence applies:

- 1. this Agreement;
- 2. Schedule A (C4 Information Management Solutions Access Terms); and
- 3. Schedule B (Common Program Agreement),

except that, with respect to any matter relating to the collection, use, or disclosure of personal information, Schedule B prevails over this Agreement and Schedule A.

In consideration of being granted access to the C4 Information Management Solutions, the Participant agrees to be bound by the access terms in Schedule A and the Common Program terms in Schedule B, each forming a part of this Agreement.

SIGNED and **DATED** with effect as of the Effective Date by and between:.

[Name of Participant]

City of Vancouver

Per: _____

Per _____

Print Name: _____

Francie J. Connell

Title: _____

City Solicitor and Director of Legal Services

SCHEDULE A

C4 INFORMATION MANAGEMENT SOLUTIONS TERMS AND CONDITIONS

In this Schedule A and in Schedule B, terms defined on the front page of this Agreement have the meanings given there. The following additional terms apply throughout:

1. DEFINITIONS

- 1.1. In this Agreement, unless something in the subject matter or context is inconsistent therewith, the capitalized terms herein will have the meanings set out below:
- (a) **“Authorized Users”** means a member of Participant Personnel who has been granted access credentials to one or more of the C4 Information Management Solutions by the Participant;
 - (b) **“C4 Information”** means, collectively, the City Information, Participant Contributed Content, and Derived Data;
 - (c) **“C4 Information Management Solutions”** means the digital tools to which the Participant is granted access under this Agreement, consisting of one or more of SharePoint, VanORCA, Unity Lens, and Common Operating Platform;
 - (d) **“C4 Structure”** means the command, control, coordination and communication structure established and operated by the City and other partner organizations to coordinate the planning and operational delivery of FWC26 in Vancouver, as listed in Appendix 1 to this Agreement, as updated by the City from time to time by written notice to the Participant;
 - (e) **“City EOC”** means the City of Vancouver Emergency Operations Centre operated by the City in connection with FWC26;
 - (f) **“City Information”** means all information the City makes available through the C4 Information Management Solutions, including Derived Data and the information the City has obtained from third party providers in connection with FWC26, but excluding Participant Contributed Content;
 - (g) **“Derived Data”** means output generated through the operation of the C4 Information Management Solutions, including alerts, push notifications consolidated data feeds, analytical results, and situational awareness displays.
 - (h) **“FIPPA”** means the *British Columbia Freedom of Information and Protection of Privacy Act*, R.S.B.C.1996,c.165;
 - (i) **“Operations Centre”** means the operational facility from which non-City EOC participants access the C4 Information Management Solutions in connection with FWC26 as listed in Appendix 1;
 - (j) **“Participant Contributed Content”** means, collectively, the SharePoint Contributed Content and VanORCA Contributed Content;
 - (k) **“Participant Personnel”** means employees, contractors, consultants, liaison officers, and volunteers acting under the direction or authority of the Participant in connection with FWC26;

- (l) **"Permitted Purpose"** means access and use of the C4 Information Management Solutions solely to support the planning and operational delivery of FWC26 in the City of Vancouver.
- (m) **"Personal Information"** has the meaning given to it in FIPPA;
- (n) **"Security Incident"** means any actual or suspected unauthorized access to the C4 Information Management Solutions, unauthorized use or disclosure of C4 Information, or any breach or suspected breach of this Agreement by the Participant or its Authorized Users;
- (o) **"SharePoint Contributed Content"** means the documents the Participant is permitted to upload to its authorized SharePoint folders, comprised of official plans and records, operational maps, operational contact lists and call trees, joint media releases, operational templates, and other non-sensitive working documents relevant to FWC26 operational coordination; and
- (p) **"Term"** means the period from the Effective Date until July 21, 2026, or such earlier date as the City specifies by written notice.
- (q) **"VanORCA Contributed Content"** means all operational data submitted by the Participant through VanORCA within the scope of the Participant's access granted under this Agreement.

2. ACCESS GRANT AND AUTHORIZED USERS

- 2.1. **Grant of Access.** The City grants the Participant a limited, non-exclusive, non-transferable right to access the C4 Information Management Solutions specified on the front page of this Agreement, solely for the Permitted Purpose during the Term.
- 2.2. **Authorized Users.** The Participant must maintain a current list of Participant Personnel to whom it has granted direct system access credentials for the C4 Information Management Solutions. The City may request a copy of the Participant's Authorized Users list at any time.
- 2.3. **Responsibility for Personnel.** The Participant is responsible for the conduct of Participant Personnel who have visibility of information or Derived Data (defined herein) through the C4 Information Management Solutions, whether through direct system access or by physical presence in the City EOC or an Operations Centre. The Participant must ensure Participant Personnel are aware of the conduct restrictions and confidentiality obligations that apply under this agreement.
- 2.4. The City may modify the Participant's access to the C4 Information Management Solutions by written notice at any time, and may suspend or revoke access immediately without notice in response to a Security Incident or operational security concern.

3. CONDUCT RESTRICTIONS

- 3.1. The Participant shall not, and shall not permit any Participant Personnel to:
 - (a) use any C4 Information Management Solution for any purpose other than the Permitted Purpose;
 - (b) access or attempt to access any part of the C4 Information Management Solutions beyond the scope recorded on the front page of this Agreement; or

- (c) copy, download, export, record, photograph, screenshot, or otherwise reproduce or redistribute any C4 Information in any form, or share any such reproduction with any person.
- 3.2. **SharePoint.** The Participant must comply with all the folder and document level permissions set by the City and must not download or export documents from SharePoint unless the City has authorized it in writing.
- 3.3. **VanORCA.** The Participant must not use VanORCA for any purpose other than sending and receiving inter-Operations Centre messages and updating its Operations Centre status dashboard, and, for participants physically present in the City EOC, such additional functions as the City make available through system configuration from time to time.
- 3.4. **Unity Lens.** Unity Lens is view only.
- 3.5. **Common Operating Platform (COP).** COP is view only.

4. CITY INFORMATION – CONFIDENTIALITY AND USE

- 4.1. **Use Restriction.** The Participant must use City Information and Participant Contributed Content accessed through the C4 Information Management Solutions only for the Permitted Purpose.
- 4.2. **Disclosure Restriction:** The Participant must not disclose C4 Information except:
 - (a) to organizations listed in Appendix 1 and their respective personnel on a strict need-to-know basis for the Permitted Purpose; or
 - (b) if disclosure to an organization not listed in Appendix 1 is necessary for the Permitted Purpose, provided that organization is bound to confidentiality obligations no less protective than those in this Agreement and disclosure is on a strict need-to-know basis only.
- 4.3. **Breach Notification.** The Participant must notify the City immediately upon becoming aware of a Security Incident involving C4 Information.
- 4.4. **Safeguards.** The Participant must take all reasonable steps to safeguard C4 Information from any unauthorized use or disclosure, including implementing and maintaining reasonable security and technological protocols and procedures appropriate to the nature of the information in the operational environment.
- 4.5. **Exceptions.** The obligations in this section do not apply to C4 Information that:
 - (a) is or becomes available to the general public other than through a breach of this Agreement;
 - (b) the Participant is required by law to disclose, provided that the Participant must, to the extent legally permitted, promptly notify the City and provide reasonable details of the request. The Participant must disclose only the minimum required C4 Information required by law and will reasonably cooperate with any lawful steps the City requests to limit disclosure or protect such information;

- (c) is obtained by the Participant from a third party who has a valid right to disclose it and who is not under a confidentiality obligation to the City in respect of it;
 - (d) is independently developed by the Participant's own employees, agents, or consultants without use of or reference to C4 Information; or
 - (e) was already in the Participant's possession prior to receipt from the City under this Agreement.
- 4.6. **Continuing Confidentiality Obligations.** The obligations in this section survive the end of this Agreement and continue for as long as the relevant C4 Information remains confidential in nature. For greater clarity, in accordance with Section 3.1(c), the Participant must not, and must ensure that Participant Personnel do not, copy, record, or otherwise reproduce any C4 Information in any form during or after the Term. As no C4 Information is to be retained by the Participant or Participant Personnel, no obligation to return or destroy C4 Information arises under this Agreement.

5. PARTICIPANT CONTRIBUTED CONTENT

- 5.1. **SharePoint Uploads.** Where the City has provisioned SharePoint upload access, the Participant may upload SharePoint Contributed Content to its authorized SharePoint folders. The Participant must keep its SharePoint Contributed Content current by replacing superseded documents with the most recent version.
- 5.2. **VanORCA Inputs.** Where the City has provisioned VanORCA access, Authorized Users may submit VanORCA Contributed Content through VanORCA within the scope of functions made available to them through system configuration, which may vary depending on whether they are operating from the City EOC or an Operations Centre.
- 5.3. **Content Warranties.** In respect of each item of Participant Contributed Content uploaded, the Participant warrants that:
- (a) it has the authority to disclose the SharePoint Contributed Content to the City and other C4 Structure participants for the Permitted Purpose;
 - (b) it will not contain any Personal Information, and that any contact list or call tree will contain business contact information only; and
 - (c) in respect of SharePoint Contributed Content only,
 - 1. it is free of malware, malicious code, and content designed to disrupt, damage or interfere with the C4 Information Management Solutions or any City system; and
 - 2. it does not infringe any third-party intellectual property.
- 5.4. **Accuracy.** The Participant must ensure that, to the best of its knowledge, all Participant Contributed Content is accurate and current at the time of upload or input and must notify the City immediately upon becoming aware of any inaccuracy.
- 5.5. **Licence.** The Participant hereby grants the City a non-exclusive, royalty free licence to ingest, process, transform, analyze, use, reproduce, store, retain, display, and make available for retrieval Participant-Contributed Content within the C4 Information Management Solutions and other City-controlled systems used to operate the C4

Information Management Solutions, in order to (a) generate Derived Data, and (b) support the Permitted Purpose, and to share Derived Data with C4 Structure participants, in each case solely for the Permitted Purpose and subject at all times to the access, confidentiality, and use restrictions in this Agreement. Following the end of the Term, the City may retain copies of the Participant Contributed Content and Derived Data only to the extent required to meet applicable legal, audit, access-to-information, or records management obligations.

- 5.6. **Ownership of Derived Data.** All Derived Data generated through the operation of the C4 Information Management Solutions is owned exclusively by the City.

6. NO RELIANCE

- 6.1. The Participant acknowledges that the C4 Information Management Solutions are made available solely to support shared situational awareness and operational coordination. C4 Information does not constitute advice, direction, or an authoritative basis for action, and the Participant must not rely on it as such. The Participant must verify the C4 Information through its own established protocols before acting on it, and accepts all risks arising from its use of or reliance on C4 Information. Nothing in this Agreement limits or modifies the Participant's statutory obligations or decision-making authority under applicable law.

7. WARRANTIES AND LIABILITY

- 7.1. **As Is.** The C4 Information Management Solutions and C4 Information available through them are provided on an "as is" and "as available" basis. The City makes no representation or warranty, express or implied, as to the accuracy, completeness, timeliness, reliability, or fitness for purpose of the C4 Information Management Solutions or any C4 Information available through them.
- 7.2. **Exclusion of Liability.** The City is not liable to the Participant for any loss, damage, or cost arising from the Participant's access to or use of the C4 Information Management Solutions or any C4 Information available through them.
- 7.3. **Indemnity.** The Participant indemnifies and holds harmless the City and its officers, employees, and contractors from and against all losses, claims, and costs arising from any act or omission of the Participant or its Participant personnel in connection with their access to or use of the C4 Information Management Solutions, including any breach of this Agreement. This indemnity does not extend to losses arising from the City's own negligence or wilful misconduct.

8. GENERAL

- 8.1. **Term and Termination.** The Agreement commences on the Effective Date and continues until the end of the Term. The City may, by notice in writing, immediately terminate this Agreement if the Participant breaches any of the terms of this Agreement. The City may also terminate this Agreement for any reason on written notice to the Participant.
- 8.2. **Survival.** The obligations set out in this Agreement survive the termination of this Agreement.
- 8.3. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties with respect to access to the C4 Information Management Solutions. If there is

any inconsistency or conflict between the terms of this Agreement and any other agreement between the parties relating to access to the C4 Information Management Solutions, the terms of this Agreement govern.

- 8.4. **Amendment.** The terms in Schedule A and the CPA Terms in Schedule B may not be amended without the prior written consent of both parties. The City may update Appendix 1 by written notice to the Participant without requiring amending of this Agreement.
- 8.5. **Governing Law.** This Agreement is governed by, and construed in accordance with, the laws of the Province of British Columbia and the laws of Canada applicable therein. Each of the parties agree to bring any action arising out of or related to this Agreement in a court of British Columbia and the parties hereby submit to the exclusive jurisdiction of the courts of British Columbia.
- 8.6. **Notice.** 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 addresses set out on the front page of this Agreement. Notices given by personal delivery will be deemed to have been received on the date of the delivery. Notices given by overnight courier will be deemed to have been received on the next business day. Notices delivered by mail will be deemed to have been received on the third day following the date of mailing. For greater certainty, email is not valid for formal notices under this Agreement but may be used for operational communications between parties, including updates to Appendix 1 (C4 Structure Participants) by the City under section 8.4.
- 8.7. **Acceptance and Counterparts.** This Agreement is executed effective as of the Effective Date and may be executed in counterparts (including electronically), each of which will constitute an original and all of which taken together will constitute one and the same instrument.

APPENDIX 1: C4 STRUCTURE PARTICIPANTS

Ops Centre	C4 Structure Participant
Vancouver EOC / Joint Info Ctre (while in EOC)	City of Vancouver (many departments)
Vancouver EOC / Joint Info Ctre (while in EOC)	All agencies with other operations centres listed in section below
Vancouver EOC / Joint Info Ctre (while in EOC)	Ministry of Emergency Management and Climate Readiness (EMCR) (Prov Govt)
Vancouver EOC / Joint Info Ctre (while in EOC)	Ministry of Public Safety and Emergency Preparedness (Public Safety Canada) (Fed Govt)
Vancouver EOC / Joint Info Ctre (while in EOC)	Ministry of Tourism, Arts, Culture and Sport (TACS) (Prov Govt)
Vancouver EOC / Joint Info Ctre (while in EOC)	Pacific National Exhibition (PNE)
Vancouver EOC / Joint Info Ctre (while in EOC)	InLive Experiences Inc. (City Fan Fest Contractor)
Vancouver EOC / Joint Info Ctre (while in EOC)	Vancouver Fraser Port Authority (Port of Vancouver)
Vancouver EOC / Joint Info Ctre (while in EOC)	Metro Vancouver Regional District (MVRD)
Vancouver EOC / Joint Info Ctre (while in EOC)	University of British Columbia (UBC)
Vancouver EOC / Joint Info Ctre (while in EOC)	Health rep could be: Ministry of Health, Vancouver Coastal Health Authority (VCH), Fraser Health Authority (FHA), Providence Health Care Society (PHC), Provincial Health Services Authority (PHSA)
Vancouver EOC / Joint Info Ctre (while in EOC)	E-Comm Emergency Communications for British Columbia Incorporated (E-Comm 9-1-1)
Vancouver EOC / Joint Info Ctre (while in EOC)	British Columbia Hydro and Power Authority (BC Hydro)
Vancouver EOC / Joint Info Ctre (while in EOC)	FortisBC Energy Inc. (FortisBC)
Vancouver EOC / Joint Info Ctre (while in EOC)	Department of the Environment / Environment and Climate Change Canada (Environment Canada) (Fed Govt)
Vancouver EOC / Joint Info Ctre (while in EOC)	The Corporation of the City of Richmond
Vancouver EOC / Joint Info Ctre (while in EOC)	Vancouver Airport Authority (YVR Airport)
Vancouver EOC / Joint Info Ctre (while in EOC)	British Columbia Rapid Transit Company Ltd. (BCRTC) (Translink operations entity)
Vancouver EOC / Joint Info Ctre (while in EOC)	Coast Mountain Bus Company Ltd. (CMBC) (Translink operations entity)
Vancouver EOC / Joint Info Ctre (while in EOC)	Universal Traffic (2026) Ltd. (traffic contractor)
Vancouver EOC / Joint Info Ctre (while in EOC)	Paladin Security Group Ltd. (CCTV security contractor to City of Vancouver)
Vancouver EOC / Joint Info Ctre (while in EOC)	Fédération Internationale de Football Association (FIFA) (as part of Mobility Branch)
Non-City Operations Centres	
VPD DOC	Vancouver Police Department (VPD)
RCMP FCC	Royal Canadian Mounted Police (RCMP)
MVTP DOC	South Coast British Columbia Transportation Authority Police Service (Metro Vancouver Transit Police (MVTP))
BCEHS District EOC	British Columbia Emergency Health Services (BCEHS)

Stadium Ops Centre (BC Place)	B.C. Pavillion Corporation (BC Place / PAVCO)
Translink EOC	South Coast British Columbia Transportation Authority (Translink)
Airport YVR	Vancouver Airport Authority (YVR Airport)
FIFA FanFest Opeations Hub FFOH (PNE)	Pacific National Exhibition (PNE)
Regional Health Authority EOC (VCH)	Vancouver Costal Health (VCH)
Training Site Killarney (security office - Paladin)	City of Vancouver
Training Site UBC (security office - Paladin)	City of Vancouver, University of British Columbia (UBC)

APPENDIX 2 CPA PARTICIPANTS

Governance Participants

1. City of Vancouver (the City):
2. Vancouver Police Department (VPD):

Operational Participants:

1. University of British Columbia (UBC):
2. Pacific National Exhibition (PNE):
3. Fédération Internationale de Football Association (FIFA):
4. B.C. Pavillion Corporation (PavCo):
5. Ministry of Emergency Management and Climate Readiness (EMCR):
6. Metro Vancouver Regional District (MVRD):
 - a. Metro Vancouver Emergency Management
7. City of North Vancouver
 - a. North Shore Emergency Management:
8. The Corporation of the City of Richmond
 - a. City of Richmond Emergency Management:
9. Ministry of Public Safety and Emergency Services (Public Safety Canada):
10. Ministry of Tourism, Arts, Culture, and Sport (TACS):
11. Department of Environment and Climate Change Canada:
12. Department of Industry (Innovation, Science and Economic Development Canada (ISED))
13. South Coast British Columbia Transportation Authority (Translink)
 - a. British Columbia Rapid Transit Company Ltd. (BCRTC)
 - b. Coast Mountain Bus Company Ltd. (CMBC)
14. British Columbia Hydro and Power Authority (BC Hydro):
15. Ministry of Transportation and Transit:
16. Vancouver Fraser Port Authority (Port of Vancouver):
17. South Coast British Columbia Transportation Authority Police Service (Metro Vancouver Transit Police):
18. British Columbia Emergency Health Services (ambulance) (BCHES):
19. E-Comm Emergency Communications for British Columbia Incorporated (E-Comm 9-1-1):
20. Vancouver Fire and Rescue Services (VFRS):
21. Vancouver Airport Authority (Vancouver International Airport (YVR)):
22. Royal Canadian Mounted Police (RCMP):
23. FortisBC Energy Inc. and FortisBC Inc. (FortisBC):
24. Ministry of Health:
25. Vancouver Coastal Health (VCH):
26. Fraser Health Authority (FHA):
27. Providence Health Care Society (PHC):
28. Provincial Health Services Authority (PHSA):
 - a. Health Emergency Management BC (HEMBC):
29. Department of the Environment/Environment and Climate Change Canada (Environment Canada)

**SCHEDULE “B”
COMMON PROGRAM AGREEMENT (“CPA”)**

BACKGROUND:

- A. The Vancouver Police Department, with an address at 2120 Cambie Street, Vancouver BC, V5Z 2N4, (the “**VPD**”) 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 CPA 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. The terms of this CPA are set out in full in this Schedule B. 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 CPA through the execution of an EOC Access and Information Sharing Agreement with the City.

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 PARTICIPATION**

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 through 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, 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) any use of Program Data by that Operational Participant or its Personnel outside the Program Purpose;
 - (c) 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
 - (d) 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. In the event of a conflict between this Schedule B and any other terms of the Agreement with respect to the collection, use, or disclosure of personal information, this Schedule B prevails to the extent of the conflict.



Number	06-5000-41
Classification title	Legal Affairs and Risk Management - Security - CCTV Recordings
Retention	Event Trigger - EV+0.1 / 0 / D
Trigger	Date reviewed
OPR (COV)	COV - Office of Custody (OPR)
OPR (Park Board)	PB - Office of Custody (OPR)
OPR (VPL)	VPL - Corporate Services and Facilities
Notes	<p>Footage from cameras stationed at various civic facilities and other points in the city. Used to monitor activities for security and public safety purposes, including the protection of City assets and property from damage or theft.</p> <p>Due to the fact that these records are retained throughout the organization it is required that any user saving into this classification must ensure that security has been set correctly.</p>