Overt Video Surveillance

Purpose and Scope

The purpose of the Columbia Shuswap Regional District ("CSRD") video surveillance policy is to establish guidelines for the CSRD's use of video surveillance within its boundaries, as well as requirements regarding the access, use, disclosure, and retention of any video footage it collects.

The CSRD may use video surveillance at CSRD owned or occupied locations for one or more of the following purposes, which it considers to be authorized by ss. 26(b) and (c) of the *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c. 165 (the *"Act"*):

a) To ensure the protection of individuals, assets and property;
b) To improve public safety; and
c) To assist in the prevention and investigation of vandalism, graffiti, theft, injury to property, and public mischief.

This policy applies to any overt video surveillance system owned or operated by the CSRD that may collect personal information about identifiable individuals in any form. This policy does not apply to the following:

a) Covert video monitoring;
b) Video monitoring conducted by the RCMP or any provincial law enforcement agency; or
c) Videotaping or audio taping of CSRD Board meetings that are open to the public.

Policy Statement

The CSRD recognizes that video surveillance has a high potential to impact individual privacy and does not wish to impair personal privacy any more than is warranted to achieve its reasonable and necessary objectives.

The CSRD will ensure that its collection of personal information by way of video surveillance is in compliance with the provisions of the *Act.* The CSRD will also ensure that the access, use, disclosure, storage and retention of personal information collected through video surveillance is in accordance with the *Act.*

Definitions

Act means the *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c. 165, as amended from time to time;

Head of the *Act* means the head of the CSRD for the purposes of administering the *Act;*

Personal information means recorded information about an identifiable individual other than contact information, as defined in Schedule I to the *Act;*

Privacy Impact Assessment ("PIA") means an assessment conducted to determine if a proposed video surveillance system meets the requirements of the *Act.* For the purposes of this Policy, the PIA will largely be in the format attached to this Policy as Appendix "A";

Record includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records;

Storage Device means a videotape, computer disk or drive, computer chip or other device used to store recorded data or visual or audio information captured by a video surveillance system;

Transitory Record means, for the purposes of this Policy, records that are created to be used only for a limited period of time. In this case, records created by a CSRD video surveillance system which do not provide a basis for further investigation or permitted disclosure will be considered transitory;

Video Surveillance System means a mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing, or monitoring.

General Responsibilities

1. The Head of the *Act* for the CSRD is responsible for the overall management of the CSRD's video monitoring program.

2. The Head of the *Act* will work with Directors of CSRD Departments, other CSRD employees, or third party contractors, as applicable, to make decisions regarding the installation of video surveillance systems, to assign responsibilities for the operation and management of video surveillance systems and to ensure the procedures set out in this Policy and the requirements of the *Act* are met.

3. The Head of the *Act* or another designated CSRD employee is responsible for:
    a. Ensuring a new PIA is completed prior to the installation and use of any new video monitoring;
    b. Ensuring a PIA is created for every existing video monitoring system as soon as reasonably possible;

c. Ensuring, as part of the review of the PIA, that the collection of personal information that will result from a video surveillance system is authorized by s. 26 of the *Act;*

d. Maintaining a record of the locations of each video surveillance system and the times it is operational;

e. Maintaining a list of personnel who are authorized to access and operate each video surveillance system;

f. Ensuring notifications are posted in every location where a video surveillance system is in effect;

g. Ensuring the video surveillance systems are subject to audit procedures at regular interviews, with the concerns documented and promptly addressed.

Notification

Given the video surveillance systems result in the collection of personal information, the CSRD is subject to the notification requirements set out in the Act.

Video surveillance systems should be clearly visible and marked by clear and prominent signage so all individuals are aware of them. The signage must clearly state the purpose(s) of the use of the video monitoring system, the legal authority for the collection of personal information, and the title, business address and business telephone number of a CSRD employee who can answer questions about the collection.

An example of signage that would be compliant with the *Act* is as follows:

> This area is monitored by video surveillance cameras for purposes of public safety and law enforcement, as authorized by ss. 26(b) and (c) of the *Freedom of Information and Protection of Privacy Act*. Please direct any questions to the CSRD's Deputy Corporate Officer (or designate) at 555 Harbourfront Drive NE, Salmon Arm, BC, Telephone (250) 832-8194 during regular business hours.

Installation and Placement

1. Prior to the installation of any new video surveillance system, the CSRD will ensure the proposed benefits outweigh the privacy impacts of those who will be observed. The CSRD will also consider whether there are reasonable alternative means for achieving the objectives of each video surveillance system.

2. Video surveillance systems will not be placed in locations where there is a particularly high expectation of privacy, including bathrooms or change rooms.

3. All video surveillance systems will be configured to collect the minimum amount of personally identifying information that is possible to still enable the CSRD to achieve the purposes of the collection.

4. Video surveillance must be positioned so as to avoid capturing third party private property or looking through the windows of adjacent buildings.

5. Video surveillance will only be operational during those hours identified as necessary by the Head of the Act or designate.

Access, Storage, Use, Disclosure

1. Access to video surveillance footage is limited to the following individuals, and only in circumstances where access is reasonably necessary for the performance of that individual's duties:

    - The Chief Administrative Officer (CAO) of the CSRD;
    - The CSRD's Head of the *Act*;
    - Other CSRD employees, as directed by the CAO or the Head of the *Act;*
    - Legal counsel for the CSRD;
    - The RCMP, as authorized by the *Act* for purposes of law enforcement; and
    - Third Party Contractors, pursuant to a valid agreement for services with the CSRD in largely the format set out as Appendix "B" to this Agreement.

2. Records created by video surveillance systems that contain personal information shall be kept secure so as to avoid unauthorized access, use or disclosure. In particular, physical and/or encrypted protection must be in place to ensure secure access to all Storage Devices created by the video surveillance systems that contain personal information.

3. All personal information stored by the CSRD in conjunction with its video surveillance systems must be stored and accessed only in Canada unless an exception set out in the *Act* is applicable.

4. The CSRD will maintain detailed and current logs of all instances of access to or use of any records created by video surveillance systems which contain personal information.

5. Records created by video surveillance systems may not be publicly viewed or distributed except as authorized by the *Act.*

6. Requests for access to any records created by the video surveillance systems will be directed to the Head of the *Act* and records may only be disclosed in accordance with the *Act.*

7. The CSRD may only use and disclose records created by video surveillance systems that contain personal information in accordance with the *Act.* The CSRD may disclose records to the RCMP for the purposes of law enforcement.

8. Where the CSRD is disclosing video surveillance records containing personal information for law enforcement purposes, it will complete an information release form.

The form will indicate who took the storage device containing the information, under what authority, when it occurred, and if it will be returned or destroyed after use.

Retention and Destruction of Footage

1. Subject to section (2) below, recorded information from all video surveillance systems should be erased or destroyed every thirty (30) days as it will be considered a Transitory Record.

2. If the CSRD intends to use an individual's personal information contained in a record to make a decision that directly affects the individual, the CSRD will ensure the record containing the personal information is retained for at least one (1) year after being used so the affected individual has a reasonable opportunity to obtain access to that personal information.

3. Records and/or storage devices that are to be erased or destroyed must be securely disposed of by shredding, crushing, burning or magnetically erasing all recorded images and sounds.

Training

Where applicable and appropriate, the CSRD will incorporate this Policy into training and orientation programs for its employees or service providers. Training programs addressing employee obligations under the *Act* will be conducted as considered necessary by the Head of the *Act* for the CSRD.

Audit Procedures

The Head of the *Act* for the CSRD will ensure that all video surveillance systems are subject to audit procedures at regular intervals, with the concerns documented and promptly addressed. Audits will include the following:

- a review of the use and security of the surveillance equipment, including monitors and storage devices;
- an evaluation of whether the policy is being adhered to, including verification that records, lists and logs required by this policy are being maintained;
- review and consideration of whether each video monitoring system is accomplishing its intended purpose; and
- recommendations, where necessary, regarding the location of video surveillance systems or duration of their operation, which may include a recommendation that one or more surveillance systems are removed.

Privacy Impact Assessment

APPENDIX "A"

Video Surveillance System

PIA#*[assigned by Head of the Act]*

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our PIA Guidelines for question-specific guidance on completing a PIA.

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:			
PIA Drafter:			
Email:		Phone:	
Program Manager:			
Email:		Phone:	

1. **Description of the location where surveillance is proposed to be installed and explanation of why surveillance is necessary (please refer to any specific incidents where public safety has been threatened, or provide examples of vandalism, theft, mischief, etc.).**

2. **Will you be collecting audio or just visual information?**

3. **How long would the surveillance be in place?**

4. **Would the surveillance be operative continuously 24/hours day? If so, please explain why this is necessary. Have you considered whether more limited periods of surveillance would meet your objectives?**

5. **What are the potential impacts of the surveillance on personal privacy? Is there some way the same objectives could be achieved without using video surveillance?**

6. **How will the information be used?**

Privacy Impact Assessment

APPENDIX "A"

Video Surveillance System
PIA#*[assigned by Head of the Act]*

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

7. Storage or Access outside Canada

Please provide a brief description of whether your information can be accessed from outside Canada, for example, by a service provider that is repairing a system, or if your information is being stored outside Canada, for example, in the "cloud". If your data is stored within Canada and accessible only within Canada, please indicate this.

8. Risk Mitigation Table

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Oath of Employment; contractual terms, etc.*	*Low*	*High*
2.	*Surveillance could capture more personal information than is necessary – such as by capturing private property*		*Low*	*High*
3.	*Other:*			

9. Collection Notice: Signage/notification is required so that individuals are aware surveillance is in place, as well as the purpose and authority for collecting their personal information. Where do you propose to place this signage so that it is highly visible?

Privacy Impact Assessment

APPENDIX "A"

Video Surveillance System
PIA#*[assigned by Head of the Act]*

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

10. **Please describe the physical security measures that will be in place to protect all records generated by the surveillance?**

11. Please describe the technical security measures in place to protect the personal information generated.

12. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

NB: You will be required to maintain an access log sheet, which records who is viewing the surveillance footage and for what reason.

Part 4 – Accuracy/Correction/Retention of Personal Information

13. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

14. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

15. **If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?**

Part 5 – Further Information

16. **Does the initiative involve systematic disclosures of personal information? If yes, please explain.**

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to Privacy Office(r).

Privacy Officer/Privacy Office Representative	Signature	Date

Privacy Impact Assessment

APPENDIX "A"

Video Surveillance System
PIA#*[assigned by Head of the Act]*

Part 7 – Program Area Signatures

Program/Department Manager	Signature	Date
Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)	Signature	Date
Head of Public Body, or designate	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.

Appendix "B"

Confidentiality Agreement for Third Parties – Monitoring of Video Surveillance

THIS CONFIDENTIALITY AGREEMENT is dated this ___ day of _____20___

BETWEEN: COLUMBIA SHUSWAP REGIONAL DISTRICT
555 Harbourfront Drive NE, Salmon Arm, BC

(the "CSRD")

AND: NAME OF CONTRACTOR
ADDRESS

(the "Contractor")

AND: NAME OF CONTRACTOR'S DESIGNATED INDIVIDUAL/EMPLOYEE
Address

(the "Recipient")

WHEREAS the Contractor has entered into an agreement with the CSRD for services at _____ (the "Contract site");

AND WHEREAS the Recipient is the individual designated by the Contractor who may, from time to time, be asked by the CSRD or the Contractor to monitor recordings made by way of video surveillance at the contract site solely for the purpose of public safety and/or law enforcement as requested by the CSRD;

AND WHEREAS the CSRD requires that the Contractor and the Recipient enter into a Confidentiality Agreement prior to accessing personal information contained in the video surveillance recordings;

NOW THEREFORE, in consideration of the CSRD granting a contract for services to the Contractor and for other good and valuable consideration, the sufficiency of which is acknowledged, the Contractor and the Recipient agree as follows:

1. The Contractor does hereby designate the Recipient as the designated individual for the purposes of this agreement.

2. The Contractor agrees that adherence to this confidentiality agreement and the CSRD's video surveillance policy is the responsibility of the Contractor and the Recipient and agrees that breach of this confidentiality agreement or non-compliance of the video surveillance policy may result in contract termination.

NOW THEREFORE the Recipient agrees that:

1. They will keep all information contained in the video recordings strictly confidential and access to such recordings and associated data must be solely for the purposes of [*insert purposes*] requested by the CSRD, and only to the extent required for that purpose.

2. They will keep all video recordings and data secure, not allow access to any other individual or group, and will not make copies of any recordings or data in any format, including electronic formats, unless given written and explicit approval by the CSRD's Head of Freedom of Information and Protection of Privacy.

3. All information shared with the Recipient is governed by the *Freedom of Information and Protection of Privacy Act* (The "*Act*") and that the Recipient will abide by the terms of this Act.

4. All recordings and data provided to the Recipient must be returned to the CSRD promptly after use, must be viewed and returned within one week of receipt, and must not be destroyed by the Recipient, except as otherwise agreed to in writing by the CSRD. The Recipient must not keep any copies of such recordings and data in any format, including electronic formats.

5. They will ensure the security and integrity of the recordings and data, and will keep them in a physically secure and separate location safe from loss, alteration, destruction, intermingling with other records and data, and access by any unauthorized individuals;

6. At all times, they will take all reasonable precaution to prevent inadvertent use, copying or transferring of the data or information provided by the video recordings and will not email or otherwise transmit the recordings or data in any format;

7. They will not disclose, divulge or communicate in any way to any person, firm or corporation, including but not limited to the Contractor or any other employees of the Contractor, any information of which the Recipient becomes aware of by means of accessing such recordings and data and will observe strict secrecy in regards to that information;

8. They will promptly deliver all data and recordings, in all media formats provided, to the CSRD upon completion of any task performed by request of the CSRD.

9. All recordings and data and any information from such recordings and data shall at all times remain the exclusive property of the CSRD.

10. They will abide by the CSRD's Video Surveillance Policy as attached to this Agreement and as updated from time to time. The Recipient agrees that breach of this confidentiality agreement or non-compliance of the video surveillance policy may result in termination of the CSRD's contract with the Contractor.

11. They will immediately inform the CSRD if they receive notice that they may, or will, be legally required to disclose video recordings or data in their possession, or to disclose information regarding recordings or data. Prior to disclosing any information, the CSRD must be consulted so that, if necessary, they can attempt to prevent or limit such disclosure.

12. The Recipient's obligations under this Agreement are to remain in effect perpetually and will exist and continue in full force and effect regardless of whether the Recipient is no longer a designated individual for the Contractor or the Contractor is no longer providing the services to the CSRD.

IN WITNESS WHEREOF the parties have signed this Agreement as of the day and year above first written:

CSRD, per:

_____
CSRD Head, Freedom of Information
And Protection of Privacy

CONTRACTOR

_____
[*insert contractor name*]

RECIPIENT

_____
[*insert recipient name*]