



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

### **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:	Justice Institute of British Columbia		
PIA Drafter:			
Email:		Phone:	
Program Manager:	Julie Brown		
Email:	jbrown@jibc.ca	Phone:	604-528-5525

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

### **1. Description of the Initiative**

The Justice Institute of British Columbia (JIBC), although an institute of higher-learning, is also a semi-secure facility, frequently under threat, containing a number of areas which should be considered secure (fire arms range, secure data, and other areas). As part of an in-depth review, the decision has been made to conduct an upgrade of the site security at campuses in order to provide additional coverage of sensitive areas for live monitoring by Security Services, as well under the current privacy policy, for review in case of a detected incident.



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

---

### **2. Scope of this PIA**

This Privacy Impact Assessment covers the existing closed circuit television (CCTV) coverage and an increase in existing CCTV coverage at JIBC campuses. In general, CCTV coverage exists at all campuses at this time, but does not fully cover secure areas, nor does it cover all areas of each campus. The goal is not to cover all areas of each site, but to improve on what is existing to attempt to provide better protection. As well, many of the existing cameras are older, and reaching the end of life - these are being upgraded at the same time to new cameras, which allow for better privacy protection with masking of non-essential areas.

### **3. Related Privacy Impact Assessments**

Not applicable.

### **4. Elements of Information or Data**

CCTV will cover visual images (only) of staff, students, visitors, and others who enter the fields of view of the cameras. This is not intended, per privacy policy already on record, to intrude upon the legitimate businesses of those using each facility, but rather to identify those who do NOT have legitimate business at the facility, and allow them to be approached by Security Services to gather further information. No identifying data of the visual images will be recorded.

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

### **Part 2 – Protection of Personal Information**

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

#### **5. Storage or Access outside Canada**

No storage of data will occur outside of Canada. However, for operational purposes, the images are accessible remotely by authorized staff of the Facilities Division and the Security Services provider (Paladin). This can include access to recorded images as well as live viewing.

#### **6. Data-linking Initiative\***

<p><b>In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.</b></p>	
<p><b>1. Personal information from one database is linked or combined with personal information from another database;</b></p>	<p><b>No</b></p>
<p><b>2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;</b></p>	<p><b>No</b></p>
<p><b>3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.</b></p>	<p><b>No</b></p>
<p><b>If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.</b></p>	



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

### 7. Common or Integrated Program or Activity\*

<p><b>In FOIPPA, “common or integrated program or activity” is strictly defined. Answer the following questions to determine whether your initiative qualifies as “a common or integrated program or activity” under the Act. If you answer “yes” to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.</b></p>	
<p>1. This initiative involves a program or activity that provides a service (or services);</p>	No
<p>2. Those services are provided through:          (a) a public body and at least one other public body or agency working collaboratively to provide that service; or          (b) one public body working on behalf of one or more other public bodies or agencies;</p>	No
<p>3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.</p>	No
<p><b>Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.</b></p>	

***\* Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body’s privacy office(r) to determine how to proceed with this notification and consultation.***

***For future reference, public bodies are required to notify the OIPC of a “data-linking initiative” or a “common or integrated program or activity” in the early stages of developing the initiative, program or activity. Contact your public body’s privacy office(r) to determine how to proceed with this notification.***



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

### 8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	Type	FOIPPA Authority
1.	Service Provider (Paladin) receives email from JIBC (Facilities Division staff) requesting service	Collection	26(c)
2.	Service Provider (Paladin) emails JIBC (Facilities Division staff) back requesting more information	Disclosure	33.1(7)
3.	Service request transferred to Service Provider (Paladin) contracted by JIBC (Facilities Division)	Disclosure & Use	33.2(c) and 32(a)

### 9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	JIBC Facilities Division staff could access personal information and use or disclose it for personal purposes, e.g. release CCTV footage publically	Employment agreements; policies and procedures regarding conduct; training in FOIPPA compliance <a href="https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/training">https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/training</a>	Low	High
2.	Service Provider (Paladin) staff could access personal information and use or disclose it for personal purposes, e.g. release CCTV footage publically	Contractual requirements between JIBC and Service Provider (Paladin); employment agreements of Service Provider staff	Low	High
3.	Request to Service Provider (Paladin) may not actually be from JIBC (i.e. their email address	Implementation of identification verification procedures	Low	High



# Privacy Impact Assessment for Non-Ministry Public Bodies

## Video Surveillance (CCTV Coverage)

PIA2019 009

	may be compromised)			
4.	Personal information is compromised when transferred to the Service Provider (Paladin)	<i>Transmission is encrypted and over a secure line</i>	Low	High
5.	Improper access to CCTV footage	Use of complex password protection, training requirements and password rotation	Low	Medium
6.	Inherent risks in Service Provider (Paladin) sending personal information to JIBC via email	Service Provider developed policy to inform clients of risk and ask if they would like the information via a different medium, such as through the mail	Medium	Medium

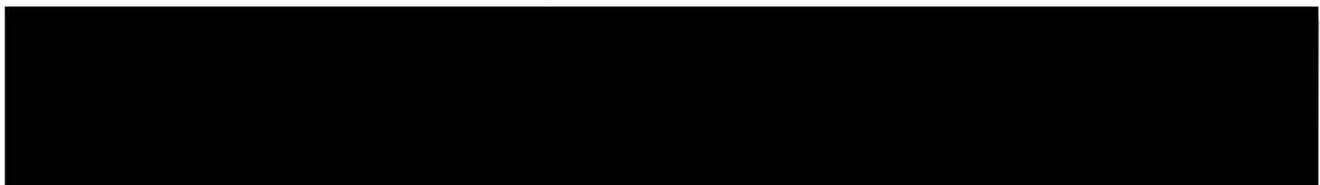
### 10. Collection Notice

Signage is in place at each campus stating the facility uses active CCTV coverage, and images may be recorded. Signs are posted at all major entrances to each campus building. New signage will be installed to add information on who to contact for any questions regarding the use of CCTV. Additional signage will be installed at entranceways once exterior cameras are in place.

### 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.***

**11. Please describe the physical security measures related to the initiative (if applicable).**





# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

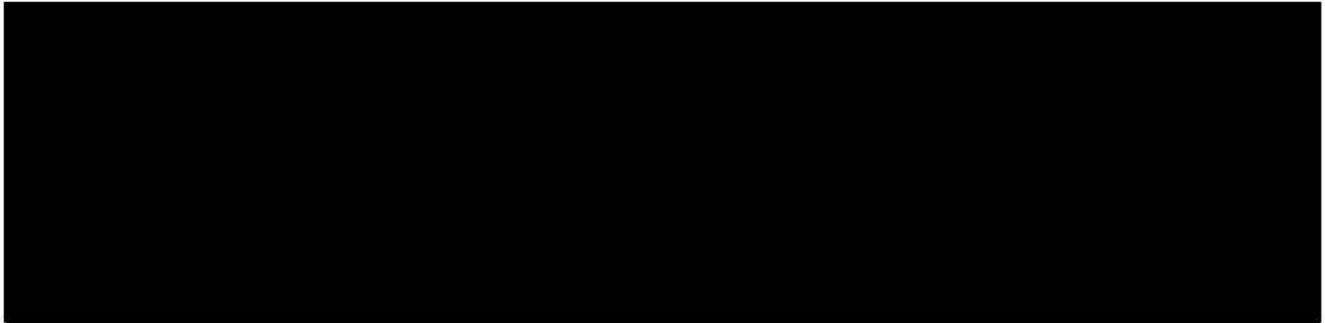
**12. Please describe the technical security measures related to the initiative (if applicable).**



**13. Does your branch/department rely on any security policies?** S.15(1)(l)

A new policy and accompanying procedure on video surveillance has been developed and is awaiting final approval. Queries regarding the policy and procedure can be directed to Julie Brown, Director, Campus Planning & Facilities Operations.

**14. 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.**



**15. Please describe how you track who has access to the personal information.** S.15(1)(l)

Only JIBC employees or contractors designated by the Director, Campus Planning & Facilities Operations or designate, shall have access to the personal information. The Director, CPFO will retain a list of JIBC employees and contractors authorized to access the CCTV system.

A monthly review of users will take place to ensure that all of the current users are authorized. The monthly review will be conducted by the Director, Campus Planning & Facilities Operations or designate, as part of a monthly preventive maintenance routine scheduled in the computerized maintenance management system (CMMS).

### **Part 4 – Accuracy/Correction/Retention of Personal Information**

**16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

Not applicable.

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

Yes, the visual data could be used to witness improper behaviour by any person recorded. The decisions made with the data could vary in results after further investigation.

**18. 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.**

Any improper activity detected by video surveillance would be responded to with further investigation by JIBC or local law enforcement. No visual information on its own will result in any further action beyond investigation.

**19. 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?**

Retention of video recordings will be recorded in the Computerized Maintenance Management System (CMMS) and scheduled for review one year in advance of the date of retention.

### **Part 5 – Further Information**

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

Not applicable.

*Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).*

**21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.**



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

Not at this time. Travel path analytics is a software option that can 'heat trace' travel or movement activities. This is not to an individual, but to general traffic patterns, and should be unrelated to the PIA.

***Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).***

**22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.**

Not applicable.

Please ensure Parts 6 and 7 are attached to your submitted PIA.



# Privacy Impact Assessment for Non-Ministry Public Bodies

## *Video Surveillance (CCTV Coverage)*

PIA2019 009

---

### **Part 6 – Privacy Office(r) Comments**

There are sufficient controls in place to mitigate the potential risks associated with the collection of these images. This initiative increases the security of staff at the JIBC.

  
\_\_\_\_\_  
Privacy Officer/Privacy Office  
Representative

*George Jones*  
\_\_\_\_\_  
Signature

*2019 April 18*  
\_\_\_\_\_  
Date



# Privacy Impact Assessment for Non-Ministry Public Bodies

## Video Surveillance (CCTV Coverage)

PIA2019 009

### Part 7 - Program Area Signatures

*[Handwritten signature]*  
JULIE BRADY  
Program/Department Manager

*[Handwritten signature]*  
Signature

*[Handwritten date]*  
April 13/19  
Date

Contact Responsible for Systems Maintenance and/or Security  
(Signature not required unless they have been involved in this PIA.)

*[Handwritten signature]*  
Signature

*[Handwritten date]*  
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.**

