A GUIDE TO THE COMPLETION OF A PRIVACY IMPACT ASSESSMENT (PIA)

What is a PIA?

A PIA is a privacy risk assessment tool that is used in identifying and assessing privacy related impacts for any system/program/legislation which collects, uses, discloses, and/or secures personal information. A PIA is also used when a change occurs to an existing system/program/legislation that collects, uses, discloses and/or secures personal information.

Why Complete a PIA?

PIA's are a legal requirement for all public bodies under S.69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). In addition to being a legal requirement, PIA's act as an "early warning system" by identifying deficiencies with regards to privacy protection. It can assist management in making informed decisions and avoid privacy breaches by ensuring an organization is complying with *FIPPA*. The PIA demonstrates accountability by including privacy as part of the design of new initiatives or systems. When designing a new initiative or program with privacy in mind, unnecessary costs are avoided throughout the process as it is inclusive from the beginning. Initiatives cannot proceed to implementation without completion and formal signoff of a PIA.

When to Complete a PIA?

PIA's should be drafted during the initial development stage of any new system/program/legislation. PIA's should also be drafted for *amendments* to existing programs/systems/legislation that detail the privacy impacts of the changes. In many circumstances, the PIA is an evolving document that becomes more detailed over time as the initiative progresses.

If the initiative involves data-linking or a common or integrated program or activity, as defined by *FIPPA,* the Office of the Information and Privacy Commissioner of British Columbia (OIPC) must be notified at an early stage in the development of the document by UFV's Privacy Consultant.

The PIA must be completed and signed off prior to the implementation of a new initiative or "launch" date of a new system or program.

Who is Responsible for a PIA:

PIA's should be drafted by the program area project manager responsible for the implementation of the system/program/legislation. Program area managers are responsible for the approval of the PIA ensuring compliance with *FIPPA* before implementation. In developing a PIA, the project manager must work closely with both Legal Counsel and the Information Technology Services department.

How to Write a PIA:

The Province of British Columbia provides a template for writing a PIA:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments

If you have any questions regarding the completion of a PIA, please contact Maureen Murphy, UFV Legal Counsel, at 604-854-4572 or Maureen.murphy@ufv.ca.

Part 1 – General

Name of Department/Branch:	Security and Emergency Management, University of the Fraser Valley		
PIA Drafter:	Mike Twolan, Manager of Security		
Email:	Mike.Twolan@ufv.ca	Phone:	604-854-4520
Program Manager:			
Email:		Phone:	

1. Description of the Initiative

This PIA will assess the closed circuit television (CCTV) system on University of the Fraser Valley (UFV) campuses for the purpose of safety and security on campus.

The current system, although limited, has proven to be very effective when used in conjunction with existing security measures. The current system deploys XX (type of cameras – fixed or pan tilt zoom cameras) cameras on various areas of the campus (see Appendix A - schematic for all camera locations that record images on campus). The images are over written every 30 days unless an incident occurs that requires an image to be copied from the system (as detailed below). Images will be stored as digital files on dedicated storage devices called Network Video Recorders (NVRs).

All cameras are mounted in plain view and are positioned in a way as to not view areas where it would be reasonable to expect privacy (change rooms, washroom facilities etc.). Cameras record images (continuously/motion activated?), but no audio recording of voices or other sounds, on a 24-hour basis and store the images as digital files on dedicated storage devices called Network Video Recorders (NVRs). Images not used to investigate or respond to an incident are overwritten on the system after 30 days without being viewed. UFV has posted signage at all main building entrances, ensuring it is clearly visible to the public, to inform individuals of the presence of CCTV cameras prior to entering into a field of view.

CCTV camera equipment, controllers, storage devices and recording information are stored on UFV premises in a secure location. Images obtained by the CCTV system can only be accessed by authorized personnel and only for the purpose of safety and security.

A party who has been subject to a CCTV recording has the right to request access to his or her personal information under the *Freedom of Information and Protection of Privacy Act* (FIPPA). In addition, law enforcement may request access to, or copies of, images on the system. Please see our law enforcement request for information form attached (Appendix D).

2. Scope of this PIA

This PIA covers all aspects of UFV's current CCTV system that will collect, use, store and disclose video footage and still images of individuals in the areas under observation by the cameras in the system. This PIA excludes any recording associated with academic purposes, weather cameras, use of equipment to record special events, interviews, public performances and any other use for broadcast for education purposes, automated teller machines, and the security call towers.

3. Related Privacy Impact Assessments

This is the first PIA on the CCTV system at UFV

4. Elements of Information or Data

- CCTV images of persons captured by cameras in the system
- Date of image capture
- Time of image capture
- Location of devices

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

No personal information will be stored or accessed outside of Canada. All video footage and still imagery obtained from the CCTV cameras will be stored on NVRs (network video recorders) and kept in secure locations on UFV campuses in British Columbia, Canada.

6. Data-linking Initiative*

In FIPPA, "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.	
1. Personal information from one database is linked or combined with personal information from another database;	NO
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	NO
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.	NO
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FIPPA, "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.	
1. This initiative involves a program or activity that provides a service (or services);	NO
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;	NO
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	NO
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

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

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	CCTV camera records still images and/or video footage of individual(s) in a specific area(s) under observation by the CCTV camera(s).	Collection	*26(b)(c)*
2.	The Director of Security and Emergency Management, Manager of Security, and/or Security Coordinators view live or recorded footage to assist in responding to and/or investigating safety and security incidents. Contracted security may also view live or recorded footage under the authority and direction of the Security & Emergency Management department.	Use	*32(a)*
3.	Once satisfied that all requirements have been met to copy images, The Director, Security & Emergency Management authorizes disclosure of copies of still images and/or video footage to law enforcement agencies for use as evidence in criminal or civil proceedings or personal injury claims resulting from a specific incident. Prior to disclosure, the Director, Security & Emergency Management makes copies of the digital files and edits them as needed to show only the image of the individual(s) under investigation. Prior to release of any still image and/or video footage, requesting law enforcement agencies must complete and sign UFV's "LEO Request for Personal Information" form.	Disclosure	*33.1(1)(i)* *33.2 (i)(i) and* *33.2 (i)(ii)*
4.	In accordance with the *Freedom of Information and Protection of Privacy Act*, the Access to Information and Protection of Privacy Office (AIPPO) may disclose copies of still images and/or video footage of individual(s) in response to their requests for access to their own personal information. Prior to disclosure, the Security and Emergency Management department will make copies of the requested digital files and edit them as directed by AIPPO to show only the image(s) of the applicant as described above.	Disclosure	*33.1(1) (a)*
5.	In accordance with the *Freedom of Information and Protection of Privacy Act*, AIPPO may disclose copies of video footage or still images of individual to third parties (other than Law Enforcement agencies) only with the written consent of the individual, or in accordance with an enactment of British	Disclosure	*33.1 (1)(a)* *33.1 (1)(c)*

	Columbia or Canada that authorises or requires disclosure. Prior to disclosure, the Director, Security & Emergency Management makes copies of the digital files and edits them as directed by AIPPO to show only the image (s) of the individual as described above.		

9. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17	Low	High
2.	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17	Low	High
3.	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17	Low	High

		s. 15(1)(l), s. 17		
4.	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17	Medium	Medium
5.	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17	Low	Medium

10. Collection Notice

You are about to enter an area that is monitored by Closed Circuit Video cameras (CCTV). The use of CCTV helps promote safety and reduce crime at UFV. Images are recorded and may be monitored for the purpose of public safety and crime prevention/detection. The personal information collected by the CCTV program is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act. For more information please contact (contact position and contact details).

Part 3 – Security of Personal Information

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

s. 15(1)(l), s. 17

s. 15(1)(l), s. 17 [redacted]

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

s. 15(1)(l), s. 17 [redacted]

13. Does your branch/department rely on any security policies?

UFV relies on both Standard Operational Procedures (SOPs) as well as UFV policy (#233) noted below in the attached link:

https://www.ufv.ca/media/assets/secretariat/policies/Closed-Circuit-Television-(233).pdf

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.

The CCTV camera system is set up so that images and recordings cannot be altered or deleted. However, in conjunction with AIPPO, the Director, Security and Emergency Management may edit a digital file in order to show only the image of the individual(s) under investigation or the individual who has requested access to his or her personal information.

The recordings are automatically deleted once a maximum of 30 days of recording has come to an end. The system then begins recording over itself. In rare cases, the system may run out of space. What is meant by this, is that the system only records when there is movement in the camera frame. More movement requires more recording space. If the recording space runs out prior to 30 days, then the system will automatically commence a new recording cycle.

15. Please describe how you track who has access to the personal information.

The Director, Security and Emergency Management or the Manager, Security or their designates, UFV Security Coordinators will be responsible for managing access to the CCTV system by adding, modifying and deleting users. The CCTV system logs all access to information in the system. Authorized users may review the audit log to identify who access information and the date, time and duration of access.

Four (4) people are authorized to export information. They are: both UFV Security Coordinators, the contracted Security Site Manager and the Supervisor for the Security Operation Center (SOC). Only these four (4) designates have the authorization and the controlled access levels to facilitate the exporting of this sensitive information. All other contracted security personnel have **VIEW ONLY** access.

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?

As the system records real time video footage updating or correcting the video images is not possible.

The Manager, Security and/or the Security Coordinators will update or correct the incident case file with any personal information obtained during the review of video footage recordings when investigating or responding to an incident.

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

Yes. Images could be used to assist law enforcement agencies, or help determine circumstances surrounding a safety or security incident.

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.

Images gained from the CCTV system are captured directly from individuals when they are in the cameras' area of observation. When CCTV footage or still images are used to further an investigation or respond to incidents, UFV Security and/or law enforcement agencies will confirm their accuracy. This can either be done by comparing the records to the individual in-person or in photograph.

19. If you answered "yes" to question 17, do you have 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?

No. When an incident occurs, the recordings are reviewed. If this incident is pursued further, a copy of the recording will be made and retained until a resolution is found or for a minimum of one year.

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

No.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact UFV's Legal Counsel.	

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

No.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact UFV's legal counsel.	

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 FIPPA. Under this same section, this information is required to be published in a public directory.

No.

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

Part 6 – AIPPO Comments

This PIA is based on a review of the material provided to AIPPO 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 AIPPO.

Maureen Murphy Legal Counsel University of the Fraser Valley	Signature	Date

Part 7 – Program Area Signatures

Director, Security and Emergency Management University of the Fraser Valley	Signature	Date
Mike Twolan Manager, Security University of the Fraser Valley	Signature	Date
Darin Lee Chief Information Officer University of the Fraser Valley	Signature	Date
Jackie Hogan Chief Financial Officer and Vice-President Administration University of the Fraser Valley	Signature	Date

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