Privacy Impact Assessment

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Campus Optics
Organization:	University of the Fraser Valley
Branch or unit:	Safety and Security
Your name and title:	
Your work phone:	
Your email:	
Initiative Lead name and title:	
Initiative Lead phone:	
Initiative Lead email:	
Privacy Officer:	
Privacy Officer phone:	
Privacy Officer email:	

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
NO
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
NO
Related PIAs, if any:

1. What is the initiative?

UFV Response:

CampusOptics is a comprehensive campus safety solution designed specifically for higher education institutions to help campus safety professionals improve collaboration, reduce institutional risk and enhance safety culture.

The intention of EHS is to use this system in the immediate future for three main purposes, for all campuses:

a. To manage safety inspections conducted by Joint Occupational Health and Safety Committees (JOHSCs).
b. To provide a centralized chemical inventory with associated Safety Data Sheets {SDS).
c. To track incidents occurring and receive data that will assist EHS in identifying trends.

However, after the system is implemented for these purposes, there may be identified other uses for the system, such as to provide the ability to track other types of safety activities, for example, equipment inspections and instrument calibration.

The adoption of the CampusOptics application will provide UFV with a better understanding of key areas of risk associated with buildings, safety systems including asset location and inspection history and to implement remediation strategies in a timely and effective manner. The incident tracking feature will not be used, since Cority, another software platform manages this.

s. 15(1)(l), s. 17, s. 21 [redacted]

Safety Inspections

The platform will manage and map key assets across UFV Campuses, log safety issues and remediation and allow personnel to conduct safety inspections. The application will allow appropriate individuals to receive notifications for action items related to safety inspections. Reports can also be generated from the system to identify information such as how many safety inspections were conducted for a department, or how many outstanding action items there are.

Manage chemical and hazardous material inventory

CampusOptics will allow UFV to track inventories and associated safety data sheets for all hazardous materials and chemicals on campus. The application will automatically request chemical quantity verifications and map containers by building, floor and area.

Incident Management

This platform will allow UFV to log key incident data including incident type, root causes, property damage and injury information.

CampusOptics Administrative Role

For the initial start-up of the application, csv files will be provided by EHS to CampusOptics of employee names, employee contact information, building information, chemical inventories and SDSs. Employees who require specific administrative access, such as those in the EHS dept. will be identified to CampusOptics and provided access. After initial start-up, it's not anticipated that CampusOptics will play an administrative role.

EHS, Administrative Role

- Provides CampusOptics with building information (including addresses) to create building maps within Campus Optics, assets data, chemical inventory (including location).
- CampusOptics provides training on how to use the application to EHS.
- Manages user rights and permissions for employees e.g., JOHSC members may require different access from other employees.
- Creates user profiles for employees and the processes on how to use CampusOptics
- Provides communication and education/training, as needed, to the UFV community

Mobile App

When a UFV employee downloads the CampusOptics Mobile App from Apple or Google Play Store, they would enter the site name they wish to be associated with (eg., UFV). CampusOptics associate the login parameters (SSO or not) to each client site.

When a user attempts to login onto a site using SSO, a browser window is launched connecting that user directly to the UFV authentication service, so their login information never passes through CampusOptics. Once the user is successfully logged in, a token is passed from UFV's authentication service to CampusOptics authenticating the user.

CampusOptics High Level Illustration of Functions:

[redacted]

s. 21

area.

s. 21

s. 21

Sample Asset Information View (Desktop View):

s. 21

Sample Mobile App Building Information View:

s. 21

[redacted]

2. What is the scope of the PIA?

UFV Response: This PIA examines the implementation and use of CampusOptics platform and app at UFV and includes the following:

- Privacy and security of the CampusOptics platform and app at UFV
- Data collection, use and disclosure between CampusOptics and UFV
- Retention and disposition of data related to the use of the CampusOptics

3. What are the data or information elements involved in your initiative?

UFV Response:

The EHS Administrators will be responsible for updating permission levels as needed, for example, if there is a new JOHSC member, they are added to the safety inspection part of the system, or if one of the JOHSC members leave, they would be removed. The HSE Division Administrator, would also keep the safety inspection templates current, for example, to add or delete line items. If buildings are built or demolished, these changes would also be reflected in the system by EHS.

Information provided by EHS to Campus Optics to create employee profile

- first name
- last name
- work email
- work phone number
- job title
- department
- assigned permissions

Employees do not set up their profiles, CampusOptics and EHS does. Employees with access to desktop system will use Single Sign-On and use UFV credentials to login or use the mobile app.

UFV Employee

Employees login to system via cell phone using UFV credentials, either as a direct link or through the mobile app. A link may also be provided via email to a certain view of the system which doesn't require login, but this view is secured such as there is no way to navigate to any other part of the system.

Access to information is dependant on permissions assigned e.g., Joint Occupational Health and Safety Committee Members for safety inspections will have access to the safety inspection section. Access to general information such as Safety Data sheets would be made available to all users.

As a user of the CampusOptics, application employees will have access to the following information:

- All employees can capture and share images of issues or concerns
- All users can view informational videos, maps and coordinates
- All users can view chemical names, basic chemical information and safety data sheets
- All users can access Inspection checklists built right into the system.
- Bar code/QR code scanning for immediate access to asset or data sheet information is available.

3.1 Did you list personal information in question 3? Yes

UFV Response: Yes

4. How will you reduce the risk of unintentionally collecting personal information?

UFV Response: Not Applicable

PART 2: COLLECTION, USE AND DISCLOSURE

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use or disclosure	FOIPPA authority	Other legal authority
Step 1: A csv file with all in scope employees information – including first and last name, work email, work phone number, job title, department for basic access is provided to CampusOptics via Dropbox to configure the system. All employees are provided with a base level of access. Dropbox can be secured by password if required.	Collection		
Step 2: A csv file with employee first and last name, indicating permission levels, is provided to CampusOptics to further configure the system. This is a select list of employees.	Collection		
Step 3: Chemical inventories, Safety Data Sheets (SDS), and safety inspection templates are provided to CampusOptics to configure the system.	N/A		
Step 4: A system for regularly updating employee information in CampusOptics is provided by Active Directory or from Banner (unknown at this point, how exactly it will occur- ITS to determine).	Collection		
EHS will be able to view the entire system and to			

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
assign and maintain permission levels.			
Employees can download the CampusOptics App from the App Store or Google Play to access mobile features such as the online safety inspection forms.	N/A		
All users will have a limited view of the chemical inventory and Safety Data Sheets (SDS). Users that are assigned an issue for remediation can still be prompted to login if they have an account. If a user doesn't have an account, they receive a "private link" from the system that allows them to view the assigned issue and enter their corrective action.	N/A		
JOHSC members will be able to view the Safety Inspection sections, and able to provide updates within their permissions.	N/A		
Designated employees from departments with chemical inventories will be able to update their own inventories within their permissions	N/A		

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

UFV Response: Not Included

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

UFV Response: No Collection Notice Required

PART 3: STORING PERSONAL INFORMATION

7. **Is any personal information stored outside of Canada?**

Type “yes” or “no” to indicate your response.

UFV Response: No

8. **Does your initiative involve sensitive personal information?**

See Guidance on Disclosures Outside of Canada
Type “yes” or “no” to indicate your response.
If yes, go to question 9
If no, go to question 10

UFV Response: No

9. **Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)? No**

Type “yes” or “no” to indicate your response.
If yes, go to question 10
If no, go to Part 4

UFV Response: Not Applicable

10. **Where are you storing the personal information involved in your initiative?**

After you answer this question go to Part 5.

UFV Response: [redacted]

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

UFV Response: Not Applicable

11. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.
If yes, fill in the table below (add more rows if necessary) and go to question 13
If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

UFV Response: Not Applicable

13. Does the contract you rely on include privacy-related terms? No

Type "yes" or "no" to indicate your response.
If yes, describe the contractual measures related to your initiative.

UFV Response: Not Applicable

15. What controls are in place to prevent unauthorized access to sensitive personal information?

UFV Response: Not Applicable

16. Provide details about how you will track access to sensitive personal information.

UFV Response: Not Applicable

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response** **(this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk?** **If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

18. Does your initiative involve digital tools, databases or information systems? Yes

Type “yes” or “no” to indicate your response.
If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

UFV Response: [redacted]

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Type “yes” or “no” to indicate your response.
If yes, you may want to append the security assessment to this PIA. Go to question 20
If no, go to question 19

UFV Response: [redacted]

19. What technical and physical security do you have in place to protect personal information?

Describe where the digital records for your initiative are stored (e.g. on your organization’s LAN, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords, encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.
If you have completed a security assessment, you may want to append it to the PIA.

UFV Response:

s. 15(1)(l), s. 17, s. 21 [redacted].

s. 15(1)(l), s. 17, s. 21 [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l) [redacted]
s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l), s. 17, s. 21 [redacted]
s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l) [redacted]

Strategy	
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

We have a process in place to correct personal information

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

UFV Response:

The information on employees is sourced from Banner or Active Directory. The data in Active Directory is sourced from Banner, so changes to the Campus Optics relevant attributes in the Banner record will be updated in Active Directory. Employees have the ability through Banner to change or update their personal information that has been provided. To do so, they simply must log in to their account, go to the profile section, and there will be options available to edit the information that they have previously submitted.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Type “yes” or “no” to indicate your response.

UFV Response: Yes

22.2 Sometimes it’s not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you’re not able to correct the record itself. Will you document the request to correct or annotate the record?

Type “yes” or “no” to indicate your response.

UFV Response: Yes

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type “yes” or “no” to indicate your response.

UFV Response: Yes

23. Does your initiative use personal information to make decisions that directly affect an individual?

Type “yes” or “no” to indicate your response.
If yes, go to question 25
If no, skip ahead to Part 7

UFV Response: No

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

Type “yes” or “no” to indicate your response.
If no, describe how you will ensure the information will be kept for a minimum of one year after it’s used to make a decision that directly affects an individual.

UFV Response:

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

Type “yes” or “no” to indicate your response.
If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA
UFV Response: NO

26. Will your initiative result in a personal information bank?

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.
Type “yes” or “no” to indicate your response.
If yes, please complete the table below.
UFV Response: NO

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the PIB

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible risk	Response
Risk 1: s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l), s. 17, s. 21 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
Risk 2: s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l), s. 17 [redacted]

Possible risk	Response
	s. 15(1)(l), s. 17, s. 21 [redacted]
Risk 3: s. 15(1)(l), s. 17, s. 21 [redacted]	s. 15(1)(l), s. 17, s. 21 [redacted]
Risk 4:	s. 15(1)(l), s. 17, s. 21 [redacted]

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative			

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security			

Role	Name	Electronic signature	Date signed
Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved			