

PRIVACY IMPACT ASSESSMENT

PART 1: GENERAL INFORMATION

Initiative Title:	Parklane Software
Approval by Privacy Office:	Yes
Brief Description	Ability management solution for all Camosun employees.
Department:	Human Resources
Dean or Director Name, Title, and Email:	Andrew Peterkin, Abilities Management Specialist John D'Agnolo, Executive Director, HR
Privacy Officer Assigned:	Ann Behennah
Product Name (if applicable):	Parklane Systems
Third Party Contact Name and Email:	Parklane Systems – Occupational Health and Safety Software Solutions - m.mihichuk@parklanesys.com
Third Party URL:	https://www.parklanesys.com/
Date of PIA:	February 21, 2025

- Describe the initiative:
 - Background:** The Human Resources Department requires specific software to use internally to manage abilities claims. Currently staff health files/claims are being managed on an Excel spreadsheet stored in a shared drive folder. The spreadsheet does not accommodate sufficient information capture and does not support procedures.
 - Goals:** To effectively and appropriately manage staff health claims, confidential information, storage of claims and track timelines related to claims.
 - Scope:** The procurement and implementation of a disability management solution for all Camosun employees.
 - Timeline:** Fall 2024 and complete implementation during Winter 2025
- Is this an administrative/operational, teaching and learning, or a research initiative? Select all that apply.
 - ☒ Administrative/Operational
- Has a PIA previously been completed for this initiative?
 - ☒ No
- What activities will occur within the initiative?
 - Personal information is being used internally to manage abilities claims.
 - The data is not digitally shared outside of HR.

Andrew Peterkin Commentary:

- If it is medical, unless an employee on a medical leave divulges any personal information, I am never apprised of any confidential medical information and if that employee were to share some information with me, it is not recorded and put in their files, I view those exchanges as confidential discussions that are not meant for anyone's viewing therefor not recorded anywhere.
- Our third-party insurer, Manulife, shares only prognosis with me, never diagnosis.

5. Describe the nature of the personal Information being used:

- Personnel file from Colleague
- Confidential information related to the abilities management claim/file of employees.
- Personal information sent to Manulife from College extends no further than civic address, phone number presented to college upon hiring, date of birth, occupation, hourly/yearly wage.

6. Did you list Personal Information in question 5? Personal Information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

☒	Yes – extensive personal info.	☐	No
Data Classification [See Appendix A]		Restricted/Limited	

PART 2: COLLECTION

FIPPA sets out rules for public bodies and their employees to collect of Personal Information. Unauthorized collection is prohibited. This section will help you identify the legal authority for **collecting** Personal Information and confirm that all Personal Information elements collected are necessary for the purpose of the initiative – section 26(c).

7. Whose Personal Information is collected in this initiative?

- ☒ Employees.

8. For what purpose will the Personal Information be used?

- ☒ It is necessary and directly related to college operations within Human Resources.

9. How will you reduce the risk of collecting unnecessary Personal Information?

- ☒ The initiative will only collect specific information deemed necessary for and directly related to the initiative. Information is loaded from Colleague – assuming a small CSV file with select records.

PART 3: USE

FIPPA sets out requirements and restrictions related to use of Personal Information. This section will help you identify the legal authority for **using** Personal Information and ensure that the use of Personal Information is limited to the original purpose for collection.

10. What is the intended use of the Personal Information collected?
- ☒ Internally in HR to manage abilities claims.
11. Does your initiative use Personal Information to make decisions that directly affect an individual?
- ☒ Yes
12. What is the intended impact of the decisions that are being made that directly affect an individual?
- ☒ Directly affects employment status, employee remuneration, or contract opportunities, and pay
13. Who will be using the Personal Information collected by this initiative?
- ☒ Human Resources

PART 4: VENDOR SECURITY, STORAGE AND PRIVACY

14. Please see attached Vendor Questionnaire (Appendix B), which states the following:

Section 15(1)(l), Section 21

PART 5: DISCLOSURE

FIPPA sets out requirements and restrictions related to disclosure of Personal Information. This section will help identify the legal authority for **disclosing** Personal Information, and consider risks related to that disclosure.

Complete this section if you are disclosing Sensitive Personal Information to be stored outside of Canada. You may need help from the Privacy Office.

- 15.** Is any Personal Information being disclosed outside of Canada under FIPPA section 33(2)(f)? This section allows for information to be made available to the public under an enactment that authorizes or requires the information to be made public.

☒ No

PART 6: PROTECTION

Please share how the initiative will secure Personal Information to protect personal privacy. People, organizations, or governments outside of your initiative should not be able to access the Personal Information you collect, use, store or disclose. You need to make sure that the Personal Information is safely secured in both physical and technical environments.

- 16. Vendor Protection:** Please see attached Vendor Questionnaire and Question 14 above.

- 17. Institution Protection and Risk Mitigation**

RISK MITIGATION TABLE				
	RISK	MITIGATION STRATEGY	LIKELIHOOD	IMPACT
1.	Unauthorized individuals could access the personal information in the system and use it or disclose it for unwanted purposes.	Standards of Conduct Policy, Acceptable Technology Use Policy, password-protected access, user access based on need to know, permission restrictions, role-based access controls, privacy training and monitoring. Camosun adheres to password standards provided by the Center for Internet Security (CIS Controls) and also use MFA for employees and contractors to further protect accounts.	Low	High

PART 7: OIPC REVIEW REQUIREMENTS (Privacy Officer to Complete)

- 18.** Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.

☒ No

- 19.** Is this initiative a common or integrated program or activity? If this PIA addresses a common or integrated program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.

☒ No

PART 13: PRIVACY OFFICE(R) COMMENTS

This PIA is based on a review of the material provided to the Privacy Office(r) as of December 16, 2024. If, in the future, any substantive changes are made to the scope of this PIA, the College will have to complete a PIA Update and submit it to Privacy Office(r). **Based upon the vendor information, this initiative contains sufficient privacy and security safeguards.**

Privacy Office Signature

Name and Title	Signature	Date signed
Ann Behennah, Privacy Office		February 21, 2025

PART 14: APPROVAL SIGNATURES

Institution Signatures

This PIA is compliant with FIPPA when it accurately documents information management practices 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 Department will inform the Privacy Office, and if necessary complete a PIA update.

By signing where required below, the signatories acknowledge and confirm their declarations as noted.

Declaration of Initiative Lead: I confirm that I understand the privacy impacts of this College initiative and I am committed to my FIPPA obligations related to the collection and management of Personal Information involved in the initiative. If there are any changes to the initiative, including to the way Personal Information is collected, used, stored, or disclosed, I understand that the department will need to inform the Privacy Office and if necessary, complete a PIA update. I will establish and document information management guidelines for the Personal Information and ensure these are followed. I will ensure employees are trained on and able to comply with their obligations under FIPPA; related College policies and procedures; and Camosun College Privacy Office recommendations relative to this initiative.

Signature of Initiative Lead or PIA Drafter

Name and Title	Signature	Date signed
Andrew Peterkin, Abilities Management Specialist	Section 22	

Declaration of Dean / Director / Budget Holder/ WPL/ One-Over-One Signatory: I confirm that I have reviewed this PIA and I acknowledge the residual privacy risks identified. I support the department by providing required time and operational resources to comply with FIPPA, related College policies and procedures, and Camosun College Privacy Office recommendations relative to this initiative.

Signature of Dean / Director/Executive Director

Name and Title	Signature	Date signed
John D'Agnolo, Executive Director, HR	Section 22	February 21, 2025

Appendix A: Data Classifications

Classification	Description
Restricted	Data of a highly sensitive or confidential nature which is intended for restricted internal use. Unintended disclosure of such information is serious and has severe or adverse effect on an individual, a group or institutional operations, assets or reputation. Access to data is generally restricted to specific legitimate use cases. Examples include: • Social Insurance Numbers • Credit Card Numbers • Health Information such as counselling notes • Security codes, access codes, or passwords
Limited	Data of a sensitive or confidential nature that is protected from general internal distribution. Unintended disclosure of such information has moderate effect on an individual, a group or institutional operations, assets or reputation. Access to data is generally limited to individuals in specific job functions. Examples include: • Course Grades and Academic Standing • Student number • Birth date • Citizenship
Internal	Data that is available to those members of the college community with a clear business need for access as part of their employment or academic duties and responsibilities. Unintended disclosure of such information has minimal or no effect on an individual, a group or institutional operations, assets or reputation. Access to data is provided based on a person's relationship with the College. Examples include: • Aggregated demographic information (from which personal information about an individual cannot be identified or inferred) • Student contact information (including email address) • Basic floor plans
Public	Data that is (or can be) generally available to all employees, the general public, and the media. Unintended disclosure of such information has no effect on an individual, a group or institutional operations, assets or reputation. NOTE: This classification does not mean that the data should be published or confirmed in all situations. Examples include: • Convocation Lists • Campus maps, parking • Student demographic data aggregated at the institutional level • Job postings



Appendix B: Vendor Questionnaire

Vendor Questionnaire

Vendor Name: **Parklane Systems Inc.**

Product Name: **Parklane**

Product Description: **OH&S Software**

Web Link to Product Privacy notice

Web Link to Accessibility Statement or VPAT

Vendor Contact Information:

**10-521 Nottinghill Rd
London, ON, Canada
N6K4L4**

Financial:

What is the total cost of ownership including subscription commitments over multiple years and implementation costs?

Section 21

Technical/Integration/Support

Is local installation required or is it Cloud base?

Cloud Based

If not Cloud based:

Does the software/system have a server or network installation component?

How many devices will require installation?

Are there any specific device requirements to run the software?

Will the system integrate with existing Camosun accounts (single sign-on, LDAP, etc.?)

Yes.

Will the system load data from any other Camosun systems, if so, is it a large volume?

Yes, a data transfer is typically done on an ongoing basis for demographics.

Will the system export data to any other Camosun systems, if so, is it a large volume?

The system can export data, but that is the preference of the client.

How will the system be supported?

Parklane will fully support the system with a Hosted Services contract and SLA including maintenance, updates and support of the software from a user perspective.

Privacy/Security

What personal data is collected, used, stored or disclosed with the use of the system? Please provide details on the disclosure, including to whom it is disclosed.

PII is defined in two categories at Parklane

"Customer Support" PII is information collected by Parklane Support to provide support services to the customer. This information includes Name, Department, Phone Number and Email Address. This information is stored in a customer file and is accessible by the Parklane Support team. If a support contact is no longer with the customer, or if a customer terminates their contract, this information is deleted.

"Application Data" PII is information entered by the customer into the Parklane System. This can include Employee Demographics and Incident data. All data residing in the Parklane System is controlled by the customer. Parklane does not access, use, process, or analyze the data contained

within the Parklane Application. Parklane has no insight into the data contained within the hosted application.

Where is this data stored/is it stored outside of Canada?

All data is stored in London, ON, Canada. Backups are stored in Woodstock, ON, Canada.

Who is the service provider that stores collected data?

Parklane Systems Inc.

Which internationally recognized standard, or framework does your organization (and/or the services provider that stores collected data) adhere to such as SOC 2, ISO 27007, PCI DWW or SOX? Please provide certification. If not, what technical and physical security is in place to protect personal information?

Section 15(1)(l), Section 21

Is it possible for a user to download data stored in the system?

Yes, if you have assigned permissions for that user to do so. You have the flexibility to grant permissions.

How do permissions and permission delegation work?

Permissions are granted based on your preferences by user.

Does your organization have a data privacy policy?

Yes.

Will a contract be in place that includes privacy-related terms?

Yes.