Privacy Impact Assessment for Non-Ministry Public Bodies

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Hoxhunt Human Risk Management Platform provided as a Software as a Service (SaaS) solution
Organization:	Camosun College
Branch or unit:	ITS
Privacy Officer:	Ann Behennah
Project Sponsor	Ted Pennell, CIO
Project Lead	Farzaan Nusserwanji, Associate Director, IT Security

1. What is the initiative?

The purpose of this project is to implement a comprehensive Security Awareness Training (SAT) program for all Camosun College employees. The initiative will aim to enhance security knowledge, reduce the risk of cyber threats, protect sensitive information, and ensure compliance with security policies and regulations.

2. What is the scope of the PIA?

Scope of the PIA is to evaluate Hoxhunt Human Risk Management Platform (provided as a Software as a Service (SaaS) solution). Hoxhunt is an employee education platform, intended to empower each platform user with the skills and confidence to recognize and respond to phishing attacks wherever they arise.

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

Within the platform, Hoxhunt shall have access to process general employee personal information (such as employee names and work email addresses), not any sensitive employee data. For more detailed information, please see Hoxhunt's Data Processing Agreement (DPA).

3.1 Did you list personal information in question 3?

Yes.

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

Hoxhunt shall only have access to employee personal information provided to them within the platform. Hoxhunt does not collect any such information itself.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and 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**
- Name - Contact Information (e.g., email address) - Department Affiliation - Authentication data from Single Sign-On (SSO) - Training completion data - Responses to phishing simulations	Collection	**Section 26(c)**- Information is collected for the purpose of managing and administering activities of the public body (e.g., cybersecurity training) **Section 26(e)** – Information is necessary for a program or activity of the public body
This information is used only for cybersecurity training and awareness. Improvement of institutional cybersecurity risk management.	Usage	**Sections 32 and 33**

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
Disclosure is limited to internal staff responsible for cybersecurity training and compliance and access is restricted to authorized personnel	Disclosure	**FOIPPA Part 3 (Protection of Privacy)**

6. Collection Notice

Not applicable as purpose and authority are communicated through internal training emails and onboarding materials, and the College has a legitimate, job-related reason for assigning the training.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Yes.

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

Hoxhunt's SaaS solution is hosted on Google Cloud EMEA, currently in Belgium. For more detailed information, please see Hoxhunt's Data Processing Agreement (DPA).

9. Does your initiative involve sensitive personal information?

No.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

10. Is personal information stored by a service provider?

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Google	Google Cloud EMEA Ltd.	EEA
Amazon	Amazon Web Services EMEA SARL	EEA
Cloudflare Inc.	Content Delivery Network ("CDN"), Domain Name System ("DNS"), and security services provider	EEA and US
MongoDB Ltd.	MongoDB database service provide hosted on Google's infrastructure	EEA
Functional Software Inc. d/b/a Sentry	Error tracking service provider	US
Zendesk Inc.	Customer support service provider	US
Merge API Inc.	Unified API integration provider	EEA
Hoxhunt Oy	Overall responsibility for the provision of the Services	EEA

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

N/A

12. Does the contract you rely on include privacy-related terms?

Hoxhunt Data Processing Agreement Appendix 1

Annex 1, Annex 2 and Annex 3 list all the controls, roles and responsibilities and personal data protection measures

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

HoxHunt SaaS agreement lists the following controls and details of each.

- Physical Access Control
- Access control to systems
- Access control to data
- Disclosure control
- Availability control
- Responsible development and usage of AI
- Training and awareness

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

N/A

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

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.**
Collection of Employee Data	Risk of overcollection or profiling beyond necessary training purposes	Low	Low	Data collected is specified in Annex 1 of DPA; only authorized data is collected. FOIPPA 26(c/e) authority applies.	Low
Third-Party Transfers (Subprocessors)	Data transferred to subprocessors in EEA and US (e.g., Google Cloud, AWS, Sentry,	Low	Low	DPA includes SCCs, adequacy decisions, and Annex 3 safeguards	Low

	Cloudflare, Zendesk)				
Use of Personal Data for Analytics	Unclear boundary between support use and analytics can lead to unauthorized secondary use	Low	Low	DPA limits use to service provision and improvement; audit logs and access control are in place. Only Camosun authorized individuals will have access to training results within Camosun.	Low

PART 5: SECURITY OF PERSONAL INFORMATION

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

Yes, provided as a Software as a Service (SaaS) solution.

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?

Yes, Hoxhunt is qualified to comply with the SOC 2 Type II standards with regards to security, availability, and confidentiality of data. Hoxhunt's latest SOC 2 Type II report is available upon request here: https://trust.hoxhunt.com/

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

Hoxhunt is qualified to comply with the SOC 2 Type II standards with regards to security, availability, and confidentiality of data. Hoxhunt's latest SOC 2 Type II report is available upon request here: https://trust.hoxhunt.com/

20. Controlling and tracking access

Strategy	
We only allow employees in certain roles access to information	Yes.
We use audit logs to see who accesses a file and when	Yes.

PART 6: ACCURACY, CORRECTION AND RETENTION

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

Hoxhunt shall only have access to employee personal information provided to them within the platform. Hoxhunt does not collect any such information itself.

22. Requests for correction

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

Yes by changing the system inputs for name and other contact information.

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

No.

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

The only decision would be to determine what further training may be offered to an individual.

PART 7: PERSONAL INFORMATION BANKS

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

No

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.

25. 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.

N/A

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

Based upon the information as presented, no concerns at this time.

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	Ann Behennah	Section 22	August 22, 2025

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	Farzaan Nusserwanji	Section 22	August 27, 2025
Program/Department Manager	Ted Pennell		August 27, 2025
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA	N/A		
Head of public body, or designate (if required)	Evan Hilchey		