PRIVACY IMPACT ASSESSMENT (PIA)
CLOSURE SUMMARY

Initiative	Hoxhunt Cybersecurity Training Platform
PIA Reference #	2025-003
PIA Completion Date	February 18, 2025
Project Sponsor	Jordan Osiowy – Cyber Security Manager
Unit	Technology Services

The purpose of a PIA is to determine whether an initiative complies with the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**") and JIBC's policies and procedures. This document is to advise that the PIA review of this initiative has been completed. The following outlines the scope, issues, legal basis and conclusions associated with this PIA.

Initiative Description & Scope

Hoxhunt is a cloud-based cybersecurity awareness platform that delivers simulated phishing campaigns and personalized training modules to JIBC employees. The platform aims to increase awareness of cybersecurity risks and promote best practices in information security.

The system collects limited personal information to deliver and track training outcomes for employees. Business contact information (such as work email addresses) is used to deliver training, while performance metrics (e.g., simulated phishing click rates, training completions) are tracked to assess user engagement and security posture improvements.

Information Reviewed

This review is based on:

- the completed PIA Questionnaire (attached as Schedule A);
- consultation with Technology Services regarding storage locations, data flow, and user access levels;
- correspondence with the Cyber Security Manager.

Legal Basis - Privacy

Hoxhunt involves the use of existing business contact information and training performance data relating to employees. While no new sensitive personal information is collected, performance outcomes (e.g., training scores) may be viewed as evaluative data.

The collection and use of this information is permitted under section 26(c) of FIPPA, which authorizes collection necessary for an activity of a public body, namely cybersecurity awareness and compliance training.

Hoxhunt stores data outside of Canada. Section 33.1 of FIPPA requires additional analysis be conducted when personal information will be stored outside of Canada. In particular, we are required to consider factors such as whether the personal information is sensitive, where and how the information is stored, the likelihood of unauthorized access, and the impact to the individual of such an event.

Current guidance from the Province of British Columbia suggests that sensitive personal information includes, but isn't limited to:

- Personal health information
- Genetic and biometric data
- Personal financial information
- Geolocation data
- Criminal records
- Racial or ethnic origin
- Sexual orientation
- Religious, philosophical or political beliefs

The personal information is not inherently sensitive, as it does not include medical, biometric, financial, or other high-risk personal information. Accordingly, a supplementary assessment is not required under section 33.1. Furthermore, risks related to unauthorized access appear to be mitigated through secure authentication, encryption, and access limitations confirmed by Technology Services.

Where personal information is used to make a decision that directly affects an individual (e.g., assessing whether a certification is current, or whether an employee has completed mandatory training), the following provisions of FIPPA must also be observed:

- Section 28 – JIBC must make reasonable efforts to ensure the personal information is accurate and complete before using it for such decisions.
- Section 31 – JIBC must retain the personal information for at least one year after it is used in such a decision to allow the individual to access it.

Legal Basis - Security

Under section 30 of FIPPA, JIBC must ensure reasonable security measures are in place. Technology Services has confirmed that:

- data in transit and at rest is encrypted;
- administrative access is restricted to a small number of Technology Services personnel;
- the platform does not store sensitive personal information;
- access from outside Canada is limited to necessary vendor support roles.

Accordingly, no additional mitigation measures are required.

Conclusions

Based on the information provided, our review concludes that Hoxhunt may be used for its intended purpose, provided that:

- performance data is handled in accordance with JIBC's internal policies;
- any material changes to scope or data sensitivity are reported and trigger a renewed PIA review.

Responsibilities

Technology Services is responsible for ensuring that:

- employees are notified of the collection and use of their information;
- any material omissions or inaccuracies in the PIA inputs are disclosed to the General Counsel;
- a new or updated PIA is submitted if significant changes to the platform occur.

If you have any questions or concerns about this PIA, please contact the General Counsel.

SCHEDULE A
PIA QUESTIONNAIRE

Please see attached.

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

for

Hoxhunt

1. Purpose of the Privacy Impact Assessment Questionnaire

This form is used by JIBC to provide a high-level overview of the potential privacy risks of a current or proposed policy, system, project, program or activity. The results of these screening questions help judge the level of potential risk, the extent to which risk mitigation strategies may be needed and when completion of a privacy impact assessment is required under the *Freedom of Information and Protection of Privacy Act* (British Columbia) (the "**Act**").

2. Privacy Questions

Questions	Answers
Does the program involve personally identifiable information (PII) (as defined by the Act)? [Y/N]	Y
Will the program involve the collection or creation of new information about individuals? [Y/N]	N
Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information? [Y/N]	Y
Will personal information about individuals be used for a purpose it is not currently used for, or in a way it is not currently used? [Y/N]	Y
Will the program require contacting individuals in ways that they may find intrusive? [Y/N]	N
Does the program have a collection notice or use policy? [Y/N]	Y

3. Technology Questions

Questions	Answers
Does this program involve the implementation of a new electronic system or use of a new application or software to support the creation, collection, updating or storing, backing-up or disposition of personal information? [Y/N]	Y
Does this program require any modifications to existing information technology (IT) systems (e.g., integration with or consolidation of other IT systems)? [Y/N]	Y
Will a new or modified electronic system change the existing business workflow? [Y/N]	N
Does the program involve the use of new technology that might be perceived as being privacy intrusive? [Y/N]	N

4. Impact Questions

Questions	Answers
What are the purpose of collection, use and/or disclosure of the personal information? [Internal/External/Both]	To train and educate employees on the threat of phishing attacks and security safety practices.
Will personal information about the same individual that was previously maintained separately now be aggregated and stored together? [Y/N]	Y
How would you describe the information classification level of the personal information? (Select all that apply) • Highly Confidential • Confidential • Public	Public Confidential (training results)
What are the type(s) of personal information? (Select all that apply) • Bio/demographic information • Academic/education Information • Employment information • Medical/health Information • Financial Information • Criminal information • Images • Opinions about individuals • Individuals' personal views and opinions • Business contact information • Personal contact information • Other	Business contact information Education information(training results)
What are the type(s) of individuals? (Select all that apply) • Prospects • Applicants • Students • Employees • Donors/alumni/other 3rd parties • Volunteers • Service providers	Employees

• Other	
How many records documenting individuals will be stored, accessed, used or disclosed? [1-1000], [1001-5000], [5,001-50,000], [50,001-100,000], [100,000+]	1,000
How many JIBC employees, volunteers and service provider employees will be able to access, collect, use or disclose the information? [1-10], [11-50], [51-100], [101-250], [251-500], [501-1,000], [1,000+]	1000+ users of the system 1-10 administrators in TS with elevated access
Is any of the information owned by another organization? [Y/N]	N

5. Probability Questions

Questions	**Answers**
Where will the information be stored? (Select all that apply) • On campus – JIBC servers • On campus – other • Off-campus – inside Canada • Off-campus – outside Canada	Off campus – outside of Canada
Is any of the information accessed from outside of Canada? [Y/N]	Y
Will personal information be transmitted? (Select only one) • Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled) • Personal information is used in a system that has connections to at least one other system • Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed • Personal information is transmitted using wireless technologies	Personal information is used in a system that has connections to at least one other system
Will a third party (e.g., vendor or service provider) have access to the information? [Y/N]	Y
Will the program result in different record keeping systems converging? [Y/N]	N