



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Why do I need to do a PIA?

Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FOIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

If you have any questions about this PIA template or FOIPPA generally, you may contact the Office of the Chief Information Officer (OCIO) at the Privacy and Access Helpline (250 356-1851). Please see our

What if my initiative does not include personal information?

Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to their privacy office(r) even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department/Branch:	Camosun College Selkirk College Vancouver Community College Vancouver Island University		
PIA Drafter:	Shirley Lew		
Email:	slew@vcc.ca	Phone:	604-871-7000 x 7007
Program Manager:	Shirley Lew		
Email:	slew@vcc.ca	Phone:	604-871-7000 x 7007

1. Description of the Initiative

Four institutions in BC – Camosun College, Vancouver Community College, Selkirk College and Vancouver Island University - are partnering to adopt and customize to their needs, an open-source software application to use as a common integrated library system. The institutions will



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

participate in a shared instance of Evergreen, an integrated library system in a shared server infrastructure environment. The shared system will replace existing, on premise proprietary integrated library systems at each institution which are maintained and licensed separately.

The BC Libraries Cooperative manages deployment and operation of Evergreen. The BC Libraries Cooperative is a limited liability corporate body registered under the Cooperative Association Act of BC. The Cooperative pursues and delivers common business solutions on behalf of members. The Cooperative is not a vendor. It is a non-profit, collaborative business solution created, operated and shared by its owners. It is owned and managed by member libraries and is governed by a democratic structure designed for scalable business operations. For the purposes of this PIA and under FIPPA, the Cooperative is defined as an organization and service provider to the four public body institutions.

Participation in Co-op services is open in a non-discriminatory manner to eligible organizations that wish to use the services of and to participate in a shared governance and maintenance model. Operating an effective enterprise-wide shared Integrated Library System requires libraries to use a harmonized, but not uniform set of common standards, protocols, and practices.

The core functions of Evergreen include the management of patron, bibliographic and other, non-personal information necessary to provide library service to the academic community. Evergreen provides standards-based integrated library system that allows each library to independently manage its own data in a shared hosted system. The system is designed to:

- Manage large sets of non-personal bibliographic data
- Manage library user records (students, faculty, employees, community users)
- Manage circulation of materials, including inventory control
- Enable search and discovery of library collections, physical and electronic
- Manage acquisitions
- Streamline the administrative processes used by libraries;

Personal information collected include student ID's, names, contact information, and other basic data necessary for providing library service. Library staff access a central application server, managed in a secure data centre, via web browser through a server-side 128-bit SSL connection. BC Libraries Cooperative administrators and technical support personnel have access to the system and are required to follow strict provisions outlined in the Cooperative's [Privacy Security Management Plan](#). The privacy and security responsibilities of the Cooperative and the public institutions, in compliance with FIPPA, are contractually outlined in the Service Management Agreement between each institution and the Co-op.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

The shared environment enables member library personnel access to a large storehouse of metadata records but access to personal records is restricted by institution. If users request services at a library not in their home institution, the system forces a *Consent to Disclose* form to be agreed to before staff can proceed with the service request. In the event that this consent is not provided, patrons can still utilize onsite library services, for which personal information exchange is not required. Further, the personal records of the four partner libraries are walled off and inaccessible by other members of Evergreen SITKA, adding another layer of segregation and security.

This PIA has gone through a number of revisions to clarify the nature of the partnership and services, based on feedback from the OIPC. The attached Appendix I provides a timeline and further context to this initiative and nature of the service model.

2. Scope of this PIA

This PIA covers the full scope of the initiative as described above.

3. Related Privacy Impact Assessments

Privacy and security has been documented in a range of policy documents managed by the BC Libraries Cooperative contained in the [Sitka Policy Manual](#). The BC Ministry of Education, Public Library Services Branch, previously developed a PIA for Sitka members, currently 85 public, post-secondary, K-12, government and special libraries.

4. Elements of Information or Data

Personal information is downloaded from each institutions' student record system. Only a minimum amount of identifying data that is needed to provide library services is downloaded. Information downloaded typically includes name, ID number, contact information, user type (e.g. student, alumni, faculty, staff, etc.), and other data that is required per institution. A comprehensive list of personal data downloaded is listed in the table below.

Borrowing history is automatically deleted after the transaction is completed, unless the library user actively opts into this service. The system will keep records for materials not returned and billed. All partner libraries have procedures in place to keep that information current, and retained only for time period necessary.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Partners may provide community borrower privileges. This data is provided to the library with permission of the community members wishing to access service. Only active borrowers are maintained on the system.

Personal data downloaded from student record systems:

Student/Employee ID number
First name, last name
Address
Email address
Phone number
Barcode
Expiration Date
User type (student, faculty, staff, etc.)
Program



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

The Co-op hosts Evergreen on servers entirely in Canada and is wholly maintained by BC Libraries Cooperative employees, all of whom reside in Canada. Data is only accessible within Canada.

6. Data-linking Initiative*

In FOIPPA, "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;	yes
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.	



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

7. Common or Integrated Program or Activity*

In FOIPPA, “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);	yes
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.	yes
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

**** Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC). Contact your public body’s privacy office(r) to determine how to proceed with this notification and consultation.***

For future reference, public bodies are required to notify the OIPC of a “data-linking initiative” or a “common or integrated program or activity” in the early stages of developing the initiative, program or activity. Contact your public body’s privacy office(r) to determine how to proceed with this notification.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

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

	Description/Purpose	Type	FOIPPA Authority
1.	<i>Library user data collected via respective student records systems. Only the data required is collected in order for users to borrow, place holds, renew and book library material and be notified when items are due or ready to be picked-up. Data also used to maintain user accounts in terms of fees for overdue or lost/damaged material.</i>	<i>Collection</i>	<i>26(a)(c)</i>
2.	<i>User requests library service which is consistent with one of the services listed above.</i>	<i>Use & Disclosure</i>	<i>32(a) 33.2(a)</i>
3.	<i>Evergreen system sends notices to library users consistent with services above:</i> <i>Ready for pick-up notices</i> <i>Due date reminders</i> <i>Overdue notices</i> <i>Fees for lost or damaged items</i>	<i>Use & Disclosure</i>	<i>32(a) 33.2(a)</i>
4.	<i>User from a partner institution requests library service consistent with services listed above, through reciprocal borrowing agreement.</i>	<i>Disclosure of personal information agreement prompted</i>	<i>32(b)</i>
4.	<i>User from partner institution consents to disclosing their personal information agreement for the purposes of obtaining library service consistent with those listed above. Staff obtains their record from the system to provide service.</i>	<i>Disclosure</i>	<i>33.1(b)</i>

9. Risk Mitigation Table



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	With a shared cloud system, personal data is stored off premises. There is risk employees could access personal information and use it inappropriately.	1. Only a minimum of identifying data required to provide library service is stored in the shared system. Once transactions are complete, data is deleted from the system automatically. Once users are no longer active, personal records are deleted from the system. 2. Staff interface has built-in blocks enforcing user consent before staff can interact with personal records of those outside of their institution. 3. Only authorized employees, through role-based access controls assigned at each institution, will have access to user records on a need-to-know basis. 4. Protection of privacy is a core professional value, reinforced through standard procedures, policies, and staff training. 5. Employees are subject to institutional policies (Code of Conduct, Respectful Workplace,	Low	Med



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

		Privacy) and provincial privacy provisions under FOIPPA.		
2.	Centralized databases may be susceptible to security threats.	System uses ISO standard protocols for information security. It employs a variety of anti-virus tools, a 3-tier application design (defence in depth) with managed firewalls and intrusion detection system, and 24/7 manned network operations centre. Audit trails are enabled for network, application and database access. Connections are via a server-side 128-bit SSL connection and enforced role-based access control. For more information, see the Cooperative's Privacy Security Management Plan .	Low	High

10. Collection Notice

The following collection notice will be posted at each institution on our websites and will be made available in print:

SITKA ILS Shared Environment & Privacy

[Library name] is part of the SITKA community of libraries using a shared instance of the Evergreen Integrated Library System (ILS). We provide library service such as the searchable Library Catalogue, holds, check-out/in, and student account management through the ILS.

As a member of SITKA, we have access to a secure, Canadian-hosted, fully supported ILS in a shared environment with other libraries in BC and Canada, via the BC Libraries Cooperative. It is a community-supported and developed system, responsive to the specific needs of our members.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

To provide this service, the ILS obtains and stores some student information (e.g. first name, last name, student number, email address, etc.) from our institution's student record system. This information is used by our library only and not viewable by other libraries in the shared ILS environment. To make use of library services at other SITKA member libraries, users will be asked for their consent before sharing their library record at these institutions.

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with your public body's privacy office(r) and/or security personnel when filling out this section. They will also be able to tell you whether you will need to complete a separate security assessment for this initiative.

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

Servers are located in 24/7 manned network operations centre (NOC) with biometric controls. In addition all servers are located in individually locked cabinets within the NOC.

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

System uses ISO standard protocols for information security. It employs a variety of anti-virus tools, a 3-tier application design (defence in depth) with managed firewalls and intrusion detection system, and 24/7 manned network operations centre. Audit trails re enabled for network, application and database access. Connections are via a server-side 128-bit SSL connection and enforced role-based access control.

Only authorized employees, through role-based access controls assigned at each institution, will have access to user records on a need-to-know basis.

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

The Co-op has an extensive Privacy and Security Management Policy which dictates a wide variety of security policies, including those related to both physical and virtual access to systems. Additional details can be had from the Co-op's Privacy and Security Officer, Scott Leslie, at scott.leslie@bc.libraries.coop.

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.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Only authorized employees, through role-based access controls assigned at each institution, will have access to user records on a need-to-know basis.

Personal records (new or updated) are downloaded from each institution's central record system and automatically uploaded to Evergreen so editing of records is not required. Personal records that meet prescribed criteria (graduates, course completion, no longer affiliated with the institution, etc.) are deleted in batches by those with administrative level permissions.

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

At the server level, detailed authentication logs store every attempted (successful and failed) login attempt to servers. In addition, detail database server logs store connections (attempted and failed), originating source and user, and commands. Within the Evergreen application, server logs allow for the deduction of which users accessed which data at particular times.

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?

Personal records (new or updated) are transferred from each institution's central record system and to Sitka Evergreen on a scheduled basis. Personal records would not be updated or corrected by library employees directly in this system. To update their personal information, users must contact the Registrar's Office or other office at their institution with the authority to edit personal records.

Library users have the ability to view their library account information, including a summary of what they currently have on loan or hold and any fines outstanding and the reasons for those fines. When logged in, they can also perform certain functions like place holds, renew material, and book material.

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



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Personal information is not used when determining access to library services. However the status of the individual (e.g. student, staff, faculty or community user) may be used to determine what loan policies apply.

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.

N/A

19. If you answered “yes” to question 17, do you have a 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?

N/A

Part 5 – Further Information

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

No.

<i>Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).</i>	
--	--

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

Statistical reports are accessible however the data is anonymized. For example, libraries track circulation data but no identifying data is attached to these reports.

<i>Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).</i>	
--	--

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



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

No.

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



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) 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 Privacy Office(r).

Surinder Aulakh

Privacy Officer/Privacy
Office Representative

Signature

FEB. 25/2019

Date



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Part 7 – Program Area Signatures

Shirley Lew

Program/Department Manager

Signature

February 13, 2019

Date

Scott Leslie

Contact Responsible for Systems Maintenance and/or Security (Signature not required unless they have been involved in this PIA.)

Signature

February 25, 2019

Date

Shirley Lew

Head of Public Body, or designate

Signature

February 13, 2019

Date

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

If you have any questions, please contact your public body's privacy office(r) or call the OCIO's Privacy and Access Helpline at 250 356-1851.



Privacy Impact Assessment for Non-Ministry Public Bodies

Evergreen Shared ILS for PSI

PIA #20190213-VCC152

Appendix I

Clarifications re: Evergreen hosting model, purpose of shared environment, and this PIA.

We appreciate the time that OIPC analysts have taken to review the PIA, and make comments and suggestions. Most of these comments and suggestions are incorporated in the most current version of the PIA. There are three points that generated greater discussion that we wish to document here.

For context, the PIA was originally reviewed by Helen Morrison, Policy Analyst, with suggestions returned to us in April 2018. Her recommendations have been incorporated. The PIA file was subsequently handed over to Jill Nevile, Policy Analyst who reviewed the document and made further recommendations to us in September 2018 to January 2019.

- 1) For the purposes of the PIA and FIPPA, BC Libraries Cooperative is deemed to be an “organization” not a public body.
- 2) At one stage, the OIPC analyst recommended that the PIA characterize the initiative as a Common or Integrated Program (CIPA). We have opted not to proceed with this recommendation for the following reasons:
 - None of the participating post secondary libraries will be hosting the software for the others. Rather, all institutions are members of the Co-op and will be consumers of the hosted service;
 - The service is hosted by a community non-profit: BC Libraries Cooperative (Co-op);
 - The service is hosted entirely from a data centre in BC.
- 3) OIPC raised questions about data sharing capability in the shared environment. Data sharing is not the objective of the initiative. The objective is for each institution to have access to shared software platform in a sustainable business and governance model. While data sharing is technically possible, it must be initiated by the student under the Reciprocal Borrowing agreement between public post-secondary institutions in BC. In these situations, there are strict procedures that must be followed.