Privacy Impact Assessment

PIA# 24-0014

INSTRUCTIONS/INFORMATION:

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.

Do I have to answer all the questions?
Sections marked as "required" must have an answer. Specify *N/A (not applicable)* if appropriate. Other sections not marked mandatory should STILL be answered if the information is known. You will be contacted to answer any questions that are deemed relevant to this assessment so it's best to be complete.

What if my initiative does not include personal information?
You still need to complete some parts of the PIA to ensure compliance with regulation. Under question "4. Elements of Information or Data", specify "*no personal information collected*". Sections that are marked as "*required*" still need to be answered.

What if I have questions?
If you have any questions about FOIPPA generally, you may contact the "*Privacy and Access Officer*" (privacy@tru.ca). For questions specific to this PIA, contact the "*Information Security Director*" (jcuzzola@tru.ca).

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	**Library integrated library system replacement (FOLIO)**		
Name of TRU Department/Branch:	Library		
PIA Drafter (you):	Michael Purcell		
Your Email:	mpurcell@tru.ca	Phone:	**250 828 5021**
Service/Vendor:	**EBSCO Publishing Inc. – our representative is Tamara Mobucon**		
Vendor Email:	778-246-0417	Phone:	**tmobuchon@ebsco.com**

Have you consulted IT Department for this Initiative/Project/Program?
Yes_____X___ _____
(*If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.*)

Part 1 – General

1. Description of the Initiative (required)

Please provide a general description of the initiative and the context in which it functions. This could include the purpose of the initiative, its benefits, the larger process (if any) that it is part of, how it functions, the parties involved, etc. We will be assessing the impacts of this initiative so please include details which help us understand its size/scale and reach.

The TRU library is in the process of acquiring a subscription to a cloud-based library management system (FOLIO). This will replace an old library system that stores information locally. All patron and bibliographic data will be stored on cloud servers. All configuration files created in the use of the Integrated Library Systems (ILS) will also be stored in the cloud.

2. Scope of this PIA (required)

This section should explain exactly what part or phase of the initiative the PIA covers and, where necessary for clarity, what it does not cover.

The scope of this PIA is to determine if is the proposed integrated library system cloud service (FOLIO) provided by EBSCO meet the necessary security standards to protect the PII it collects, and uses as per the requirements of FOIPPA.

2-1. Is this initiative recurring in a regular interval, e.g., yearly, or biennially? (required)

This will be a permanent ongoing initiative until the new ILS is eventually replaced. We envision using the FOLIO for at least five years, but possibly years longer.

3. Related Privacy Impact Assessments

Please identify any approved PIAs which cover any parts of the initiative or any previously approved PIAs for this initiative.

N/A.

4. Elements of Information or Data (required)

Please list the elements of information or data involved in the initiative. This could include name, date of birth, home address, personal email, phone number, employment history, health information, financial information, photos, personal opinions, comments/open-ended questions on a survey, or information specific to your area, e.g., stumpage totals, visitor centre stats, etc.

Please submit a copy of any relevant details for evaluation, such as questions, forms or templates used for collection purposes; or system information covering what information is collected, used, stored or shared. These will be appended to your PIA for reference.

Currently patron data for FOLIO is primarily imported from Banner. Below is the first line of a Banner report that we use to extract patron information. (The report is pipe delimited and each section between pipes is a field extracted from Banner.) The patron information in banner is collected by the registrar's office.

Individuals can approach the library desk and have a patron record setup in the ILS before we retrieve data from Banner. In that case we collect the same information as in the Banner report. This is done primarily by users from the community who are not in Banner, but can apply for a library card. If a student sets up a library card before the data from Banner is imported the patron account information will be over written by the data from Banner at the next data load.

"Campus"|"STU_ID"|"STU_ID_ALT"|"Last_Name"|"First_Name"|"Street1"|"Street2"|"Street3"|"City"|"Province"|"Post_Code"|"Nation"|"Phone"|"Email"|"Birthdate"

In the normal operation of the ILS extra information is generated and attached to user records. This includes records of items loaned to the users, bill attached to the user record if fines are incurred etc. There is also a note feature. Free form notes can be attached to user records. Typically, the note contain information directly related to borrowing. IE the patron has read and signed a laptop use agreement.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

Can your information be accessed from outside Canada (i.e. on the TRU website), or is your information being stored outside Canada (i.e. in the "cloud", or on a non-Canadian social media site)?

FOLIO is web based and can be accessed anywhere. FOLIO is hosted on AWS which is SOC 2 / Type 2 compliant hosting service.

5-1. Is a service provider(s) involved? If so, where is the provider located (e.g. Canada, U.S., or other country)? (required)

From the FOLIO HECVAT:

DCTR-02	Are you generally able to accommodate storing each institution's data within their geographic region?	Yes	EBSCO currently offers FOLIO hosting in the following AWS regions: • US-east-1 (N. Virginia) • US-west-2 (Oregon) • EU-central-1 (Frankfurt) • CA-central-1 (Montreal) • AP-northeast-1 (Tokyo) • AP-southeast—2 (Sydney) • SA-east-1 (São Paulo)\

The FOLIO service will reside in Montreal, Canada.

6. **Common or Integrated Program or Activity (required)**
   If you answer yes, please contact the *Privacy and Access Officer*

If you answer "yes" to <u>all</u> 3 of these questions, your initiative qualifies as "a common or integrated program or activity," and you must comply with requirements under FOIPPA.	
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.	no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

7. Data-linking Initiative* (required)
If you answer yes, please contact *Privacy and Access Officer*

If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
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

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information (see examples below) (required).
Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FOIPPA. If the authority comes from other legislation, please identify the applicable act(s) or regulation(s), including specific section references. Please contact Manager, FOI and Privacy for assistance on this.

Collection, Use, and Disclosure of Personal Information

Category	Description
Collection **s.26(c)(d)**	- **Data Collected**: User account details (see part 1 question 4), access logs, administrative activities. Records of items loaned, bills and fines, and notes. - **Method**: Through user interactions, API usage, Banner import, FOLIO administrative users, and system logs.
Use **s.32(a)(b)**	- **Purpose**: To provide the services of an integrated library system; to provide users the means to borrow library assets. - **Data Retention**: Data is retained for six months post-contract termination and can be provided in the form of a database extract. - **Data Deletion**: Data will be deleted from all systems and archives after the specified retention period.

Category	Description
	- **Audit Logs**: Access and administrative activities are logged, including user details, date/time, and IP addresses. **- Backups**: Full or partial data backups can be provided upon request.
Disclosure **s.33(2)(d)**	- **Legal Agreements**: Legal agreements ensure third parties adhere to security, service recoverability, and confidentiality standards. - **Access Control**: Role-based and attribute-based access control to limit data access to authorized personnel only.

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) of this risk happening and the degree of impact it would have on individuals if it occurred (insignificant, minor, moderate, major, catastrophic). You may contact the *Information Security Director* for assistance.

Privacy Risks and Mitigation Strategies for FOLIO

Privacy Risk	***Mitigation Strategy***	***Likelihood*** *(before mitigation)*	***Impact*** *(before mitigation)*	***Exposure***
s.13				

Privacy Risk	*Mitigation Strategy*	*Likelihood* (before mitigation)	*Impact* (before mitigation)	*Exposure*
s.13	[redacted]			

Privacy Risk	*Mitigation Strategy*	*Likelihood* (before mitigation)	*Impact* (before mitigation)	*Exposure*
s.13	[redacted]			

→ Exposure rating of *high* or *critical* is of concern. Please contact Director, Information Security to discuss possible solutions.

s.13 [redacted]

Risk Exposure Matrix

Risk Exposure Matrix	IMPACT				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Medium	High	Critical	Critical
Likely	Low	Medium	High	Critical	Critical
Possible	Insignificant	Low	Medium	High	High
Unlikely	Insignificant	Low	Low	Medium	Medium
Rare	Insignificant	Insignificant	Insignificant	Low	Low

10. Collection Notice

If your initiative collects personal information directly from any individuals, you must ensure that all individuals involved are told the following:

1. The purpose for which the information is being collected
2. The legal authority for collecting it, and
3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

Please contact *Privacy and Access Officer* for assistance on this.

Standard Collection Notice

Any personal information is collected by the Thompson Rivers University under *Section 26 (c)* of the *Freedom of Information and Protection of Privacy Act* and will be used to *provide loan services to library assets (books, latops, etc.) and to manage related fees and fines*. Should you have questions about the collection of this information, please contact:

Michael Purcell
Associate Librarian / TRU Library Services
Thompson Rivers University, Kamloops, BC
250 828 5021
mpurcell@tru.ca

Part 3 – Security of Personal Information

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

For example: locked cabinets, securely stored laptops, or key card access to the building.

EBSCO hosts FOLIO on the Amazon Web Services (AWS) platform and defers all physical security controls to AWS. This includes making use of AWS best practices for logical security controls. AWS is SOC 2 / Type 2 compliant.

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

For example: use of firewalls, document encryption, or user access profiles assigned on a need-to-know basis.

Technical Security Measures Related to FOLIO:

a. ***Multi-Tenant System****: FOLIO is designed as a multi-tenant system with the capability to implement solutions using dedicated instances or separate tenants within instances.*

b. ***Data Encryption****:*

- ***In Transit**: All data in transit is encrypted using TLS 1.2.*
- ***At Rest**: Sensitive data is encrypted in storage.*

c. ***Access Controls**:*

- ***Role-Based Access Control (RBAC)**: Each tenant manages its own set of user groups with defined permissions and applications access. Authorized personnel can be assigned to administrative groups.*

d. ***Audit Logs**: The FOLIO audit logging system logs all actions and data points for auditing and reporting purposes. This includes logging of all login, logout, actions performed, and source IP address.*

e. ***Web Application Firewall (WAF)**: AWS WAF is used to protect web applications.*

f. ***Intrusion Detection and Prevention**:*

- ***Network-Based Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)**: CheckPoint firewalls incorporate IDS/IPS functionality, including threat monitoring and active blocking.*
- ***Host-Based Intrusion Prevention**: Sophos endpoint protection is used.*

g. ***Next-Generation Persistent Threat (NGPT) Monitoring**: Perimeter firewalls incorporate next-gen bot detection and persistent threat monitoring and alerting.*

h. ***24/7 Intrusion Monitoring**: Amazon Web Services GuardDuty is used to monitor for unusual activity patterns in FOLIO and notify the incident response team.*

i. ***Software Supply Chain Management**: Procedures are in place for managing the software supply chain.*

j. ***Security Assessments**:*

- ***Vulnerability Scanning**: Internal and external vulnerability scans are regularly performed to monitor for and protect against common web application security vulnerabilities.*
- ***Penetration Testing**: Annual penetration tests are conducted.*

k. ***Secure Coding Practices**: Developers are trained in secure coding techniques, reinforced with code reviews and automated and manual analysis tools.*

l. ***Authentication Services**: FOLIO supports SAML authentication and can accept logins from various SAML single sign-on systems/Identity Providers, including Okta, Shibboleth, Microsoft Active Directory ADFS, Azure, and Google Suite*

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

Please describe any specific policies and procedures and provide contact details for someone who could answer questions on this matter. If you are relying on a third-party's policies, please include links or documentation for our review, if available.

EBSCO's Policies:

a. ***Patch Management Process**:*
   - *Documented process for patching legacy systems monthly and redeploying new systems to clean images.*

b. ***Encryption Requirements**:*
   - *Implements encryption using open standards such as AES-256.*

c. ***Information Security Principles**:*
   - *Security principles are integral to the product lifecycle, including security assessments prior to each software release.*

d. ***Systems Development Life Cycle (SDLC)**:*
   - *Documented SDLC available on their website.*

e. ***Breach Notification**:*
   - *Complies with applicable breach notification laws, notifying within 72 hours.*

f. ***Compliance with IT Policies**:*
   - *Will comply with the institution's IT policies regarding user privacy and data protection.*

g. ***Compliance with Privacy Laws**:*
   - *Complies with FERPA, GDPR, CCPA, and other applicable privacy laws and regulations.*

h. ***Employee Background Checks**:*
   - *Requires comprehensive background checks for all employees and contractors prior to their first day of work.*

i. ***Employee Agreements and Policy Review**:*
   - *New employees must sign an NDA and review relevant company and information security policies.*

j. ***Information Security Policy**:*
   - *Documented information security policy included in their response.*

k. ***Security Awareness Program**:*
   - *Conducts annual information security awareness training for all employees and new hires, including continuous evaluations and mandatory follow-up training.*

l. ***Physical Security Controls and Policies**:*
   - *Relies on AWS for physical security controls and follows AWS best practices for logical security controls.*

m. ***Incident Response Plan**:*
   - *Formal incident response plan to manage security issues and threats.*

n. ***Business Continuity Plan (BCP)**:*
   - *Documented BCP tested annually.*

o. ***Disaster Recovery Plan (DRP)**:*
   - *Documented and tested annually, maintaining six copies of data across three cloud data centers.*

p. ***Internal Audit Processes**:*
   - *Regular internal audits to ensure least privilege and appropriate use of resources.*

q. ***Background Screening**:*
   - *Background checks including criminal, education, work history, financial, and terrorist watch list screenings.*

r. ***Privacy Policy**:*
   - *Documented data privacy policy available online.*

s. ***Employee Onboarding and Offboarding**:*
   - *Comprehensive HR security policy covering onboarding and offboarding processes.*

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. (required)

For example: role-based access.

Access Controls and Restrictions on Unauthorized Changes to Personal Information:

a. ***Role-Based Access Control (RBAC)**:*

- *Each tenant manages its own set of user groups with a defined set of permissions and application access. Authorized personnel can be assigned to an administrative group that has administrative capabilities.*

b. ***Attribute-Based Access Control (ABAC)**:*

- *Access controls are based on structured rules, which can also be attribute-based.*

c. ***Logging and Monitoring**:*

- *The application logs record access, including specific user, date/time of access, and originating IP or device.*
- *Administrative activities, such as user account access changes and password changes, are logged, including the specific user, date/time of changes, and originating IP or device.*

d. ***System Capabilities**:*

- *The system has capabilities to log security/authorization changes as well as user and administrator security events (e.g., login failures, access denied).*
- *All privilege changes and access control events (including login and log out, change password, and login failure) are logged and events are propagated into a searchable database.*

e. ***Policy on Administrator Access**:*

- *EBSCO maintains detailed logical access control security, with employees provisioned based on job role under the principle of least privilege. Employee access to the system is requested by management and approved based on the necessity of the role.*

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

For example: audit trails or physical sign-in and sign-out of files.

Tracking Access to Personal Information:

a. ***Access Logging**:*

- *The application logs record access including specific user, date/time of access, and originating IP or device.*
- *Logs administrative activities such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device.*

b. ***Quarterly Reviews**:*

- *There are documented processes that require a review and update of the access list(s) for privileged accounts on a quarterly basis.*

c. ***Internal Audits**:*

- *Periodic reviews are conducted to ensure least privilege and appropriate use of privileged resources.*

d. ***Role-Based Access Control (RBAC)**:*

- *Each tenant manages its own set of user groups with defined permissions and application access. Authorized personnel can be assigned to administrative groups.*

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's personal information updated or corrected? If it is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated.
For example: users have access to update their own information or notes will be made on a case file.

Updating or Correcting Personal Information:

The process for updating or correcting personal information involves the following steps:

a. ***Application Logging**: The application logs access, including the specific user, date/time of access, and originating IP or device. It also logs administrative activities, such as user account access changes and password changes, including specific user, date/time of changes, and originating IP or device .*

b. ***Role-Based Access Control (RBAC)****: Each tenant manages its own set of user groups with a defined set of permissions and application access. Authorized personnel can be assigned to administrative groups with the capability to update or correct information .*

c. ***Procedures for Changes****: If personal information is not updated or corrected due to physical, procedural, or other reasons, the system logs any changes or attempts to change data. These logs provide a record of the attempts and reasons for not updating or correcting the information.*

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

NO

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.
For example: check to see that the information was obtained from a reputable source such as another government agency.

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?
If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please contact Manager, Information Services.

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.
For example: your initiative involves a regular exchange of personal information (both collection and disclosure) with other government(s) and/or other agencies in order to provide services to your clients.

N/A

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact Legal Services.	

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

For example: your initiative involves disclosing information to PhD students so that they can conduct research.

N/A

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA, please contact *Privacy and Access Officer*.	

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.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Yes, see part 1 question 4 for data elements captured.

Part 6 – Canada's Anti-Spam Legislation (CASL) Compliance

23. Please confirm if you plan on emailing, texting, or instant messaging as part of your project. (required)

N/A

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM[1])?

N/A

25. If your communication message does fall under CEM rules, you must comply with the unsubscribe mechanism and identification requirements under CASL. Please confirm your method of unsubscribe mechanism that must be processed within 10 business days and how you will meet the identification requirements?

N/A

[1] If your initiative or program sends commercial electronic messages (CEMs), such as emails promoting a product or service, you must comply with CASL's requirements to: (1) obtain consent, (2) provide identification information, and (3) include an unsubscribe mechanism in each message. Please note that an electronic message that contains a request for express consent is also considered to be a CEM under CASL.

26. If you do meet the definition of CEM, please confirm that you have a records retention schedule that will ensure that consent communications, both paper and electronic, are stored appropriately and retained for three years after the last communication?

N/A

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

(This section to be completed by the **Information Security Office**). If your initiative involves the transmission of personal data between TRU and the vendor, or from the vendor to 3rd parties, then TRU may ask for the name of the software used to determine if there are applicable CVEs.

(Info. Sec): Not Applicable. No CVEs found.

Part 8a – Information Security Director Comments

s.13 [redacted]

John Cuzzola	s.22 [redacted]	2024-07-22
Information Security Director	Signature	Date

Part 8b – Privacy Officer Comments

Privacy and Access Officer	Signature	Date

Part 9 – Program Area Signatures

Program/Department Manager	Signature	Date
John Cuzzola	s.22 [redacted]	2024-07-22
Information Security Director		Date
Senior Manager, Program Area/Division	Signature	Date
General Manager	Signature	Date
General Manager	Signature	Date

A Final Copy of this PIA (with all signatures) shall be kept on record by the program area responsible for this project. The signed original record will be retained by the FOI and Privacy Office. ***If you have any questions about FOIPPA generally, you may contact the "Privacy and Access Officer" (privacy@tru.ca). For questions specific to this PIA, contact the "Information Security Director" (jcuzzola@tru.ca).***