PRIVACY MATTERS @ UBC

PIA01421 — Transfer Credit Portal (TCP) Development Project

THE UNIVERSITY OF BRITISH COLUMBIA

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

UBC Go Global (GG) is looking to replace its existing Transfer Credit Portal (TCP) with the new TCP to support Go Global Transfer Credit processes. The current TCP, due for an update, operates on a platform that is scheduled for modernization to enhance security and functionality. This creates an urgency for Go Global to have the current application re-developed with a stable and secure environment.

Personal information of students including name, student number, email, academic and course information such as faculty, major, course model, transcripts, etc. is collected to process transfer credit and course articulations. The information will be accessed by students and authorized Go Global and Enrolment Services staff.

The new TCP is an in-house developed application. Its server is hosted at UBC Data Centre and internally managed and supported by UBC IT. TCP is implemented with the CWL integration. It is not integrated with other systems.

1.2 Project Description

The Transfer Credit Portal is used by UBC students on exchange & study abroad programs, Go Global staff, faculty designates, academic advisors, articulators and Enrolment Services staff to track and process transfer credit packages from UBC students studying abroad at partner universities.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is 4 – **High**.
The residual risk classification level of this PIA submission at closure is 3 – **Medium**.

1.3 Scope

The scope of this PIA is the implementation of Transfer Credit Portal (TCP) for direct use by UBC staff and students who are authorized to use the application on behalf of UBC.

1.4 Data Elements

TCP collects necessary academic and personal information to facilitate transfer credit processes, ensuring compliance with educational and privacy standards.

1.5 Storage or Access Outside of Canada (including back-ups and recovery)

Not applicable, TCP servers storing student data are hosted at UBC Data Centre.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under FIPPA s. (36).

1.7 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in FIPPA Schedule 1.

1.8 Related PIAs

2019.09-169

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram/Table

Not applicable.

2.2 Risk Mitigation Table

Privacy Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Unauthorized access to PI during design and development	RK0020684	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: The project includes the use of real data for testing purposes. To ensure the protection of personal information, all data utilized in non-production environments will undergo anonymization or similar protective measures to safeguard individual identities and sensitive details.				
Retaining PI longer than necessary	RK0020686	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: The project to consult with the UBC Records Management Office (RMO) to develop the records retention and destruction plan for archival data stored in the legacy TCP and data in the new TCP system and ensure to follow the established plan.				
Disclosing to or allowing unauthorized users access	RK0020685	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: To enhance data privacy and minimize exposure risks, the following measures are recommended: 1. Redact or remove any unnecessary personal identifiers displayed within the TCP interface. 2. Restrict download capabilities within TCP, ensuring that sensitive documents, such as transcripts, are view-only for users, with download permissions limited to authorized personnel only.				

Security Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020687	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Appropriate risk mitigation measures are in place to protect personal information during design, development, and operational phases, in accordance with UBC's standards and in collaboration with the respective Client Service Manager and the UBC IT /Cybersecurity Team.				

2.3 Collection Notice

UBC Students should be given a standard personal information collection notice before they provide their personal information. This discloses the legal authority to collect information, the purpose for collection, and contact information for asking for clarification.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

Not applicable, consent is not required as this project does not result in the storage of personal information outside Canada.

2.5 Consent Withheld Procedure

Not applicable, consent withheld procedures are not required as consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards). The project continuously enhances its security measures to meet UBC's rigorous standards and adapt to evolving cybersecurity threats.

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.4 Tracking Access/Access Controls

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBCISS (Information Security Standards). Student and course information will be accessed by UBC Go Global, faculty and department employees and Enrolment Services staff to process transfer credit and course articulations. The personal information collected in new TCP will not be shared with any individuals or institutions outside UBC.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Go Global and Enrolment Services have had a process to ensure the information entered in TCP is updated and accurate.

4.2 Decisions That Directly Affect an Individual

This project does not capture personal information that directly affects an individual.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies. A records retention and destruction plan has not been established for archival data stored in the legacy TCP and data in the new TCP system. It is recommended that the project consult with the UBC Records Management Office for the records retention and destruction guidelines. This observation is included in the risk mitigation table.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under FIPPA s. (35).

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Overall provided information was deemed reasonable to provide an understanding of operating privacy and security controls.

6.2 Analysis and Findings

The privacy and security risks were noted during our review. The project has accepted and agreed to implement the recommended remediate actions as outlined in the risk mitigation plan to minimize risk exposures and to comply with FIPPA and UBC Information Security Standards.

6.3 Conditions of Approval

The project to ensure the implementation of the risk mitigation actions during the implementation of Transfer Credit Portal (TCP).

6.4 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

Assessment Acceptance
Patricia Siggers

Distribution
Requestor: Sha Xiao **Project Manager**: Sha Xiao **Owner**: Patricia Siggers, Content and Engagement Strategist **Risk Advisor**: Pimkae Saisamorn, Senior Information Security Risk Analyst

PIA Request Submission	Report Completion
2020-06-02	2021-04-30