Privacy Impact Assessment
Emily Carr University of Art + Design

Blue by Explorance PIA

PIA#

Part 1 – General Information

Name of Department/Unit	Academic Affairs	**Project ID**	PROJ039- Replacing Course Evaluation System
PIA Drafter	Ali Entezari		
Email	aentezari@ecuad.ca	**Phone**	
Project Sponsor	Patricia Kelly, Sandeep Sidhu		
Email	trishkelly@ecuad.ca Sandeep@ecuad.ca	**Phone**	
Project Manager	Ahmad Al-Sharbati		
Email	aalsharbati@ecuad.ca	**Phone**	

1. What is the initiative?

Background

In 2022, Emily Carr University (ECU) launched a project to acquire a new technological solution to replace the institution's current course evaluation system.

The current course evaluation system was designed and delivered by OA Solutions for WebAdvisor (MyEC) web-portal in 2016. It was designed to have a single set of questions for all course evaluations. During Covid-19, all courses were migrated to online learning, and moving forward, some courses will continue to offer this option or have a hybrid model course curriculum. To stay relevant and meet expectations of faculty and students, a new system that is more customizable in terms of evaluation sets, survey start/end dates, more user-friendly and in line with Self-Service (ECU's new web-portal) is required. The desired outcomes of this project and new system include:

- Replacement of the Course Evaluation System for credit students (undergraduate transcriptable and graduate).

- Added functionality for non-transcriptable students. This involves certificates programs, workshop and other course work offer by Continuing Studies.
- Customization of ERP, Ellucian's Colleague, to integrate the new Course Evaluation System while maintaining existing functionality.
- Improvement of data processing and delivery workflow.

Proposed Solution

Through ECU's consultation with various post-secondary institutions in British Columbia and review of a variety of solution offerings, ECU has determined that Blue by Explorance (herein referred to as Blue) is the most appropriate solution for achieving the desired outcomes.

Blue is an online course evaluation platform designed to support organizations with their feedback gathering needs. Blue is developed by a Canadian company (Explorance) and all infrastructure and data are hosted in Montreal, Canada. Blue is currently contracted by numerous post-secondary institutions such as Simon Fraser University, British Columbia Institute of Technology, and the University of British Columbia to achieve their course evaluation requirements. Built to support the most important feedback processes, including course evaluations, Blue supports data driven decisions at all levels of the institution. Blue enables an institution to connect all central and major feedback gathering initiatives in one centralized location, including:

- Applicant feedback
- Onboarding surveys
- Teaching and learning surveys
- Midterm reviews
- Competency assessments
- Advisor assessments
- Climate surveys
- Student exit surveys
- Alumni surveys

At the time of writing, the teaching and learning surveys (otherwise referred to as course evaluation surveys) is the functionality that will be most utilized by ECU; however, other functionalities are anticipated to be integrated into ECU's business processes in the future. If so, this PIA will be updated where necessary.

Blue was created with privacy and security controls designed into the system, permitting the institution to limit the collection, use and disclosure of personal information by Blue. For example, with the ability to integrate with ECU's LDAP system for authentication and SIS for validation of students and instructors with course enrolment, Blue leverages systems and controls governed by ECU.

Figure 1: Overview of Blue's system architecture

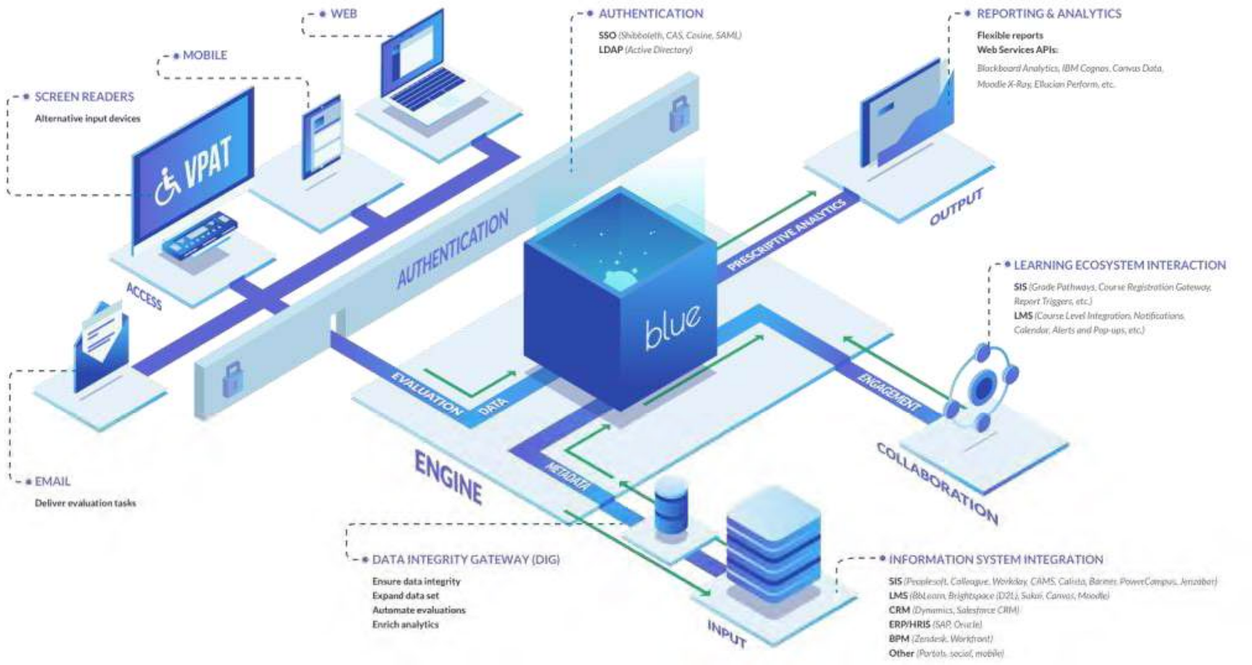
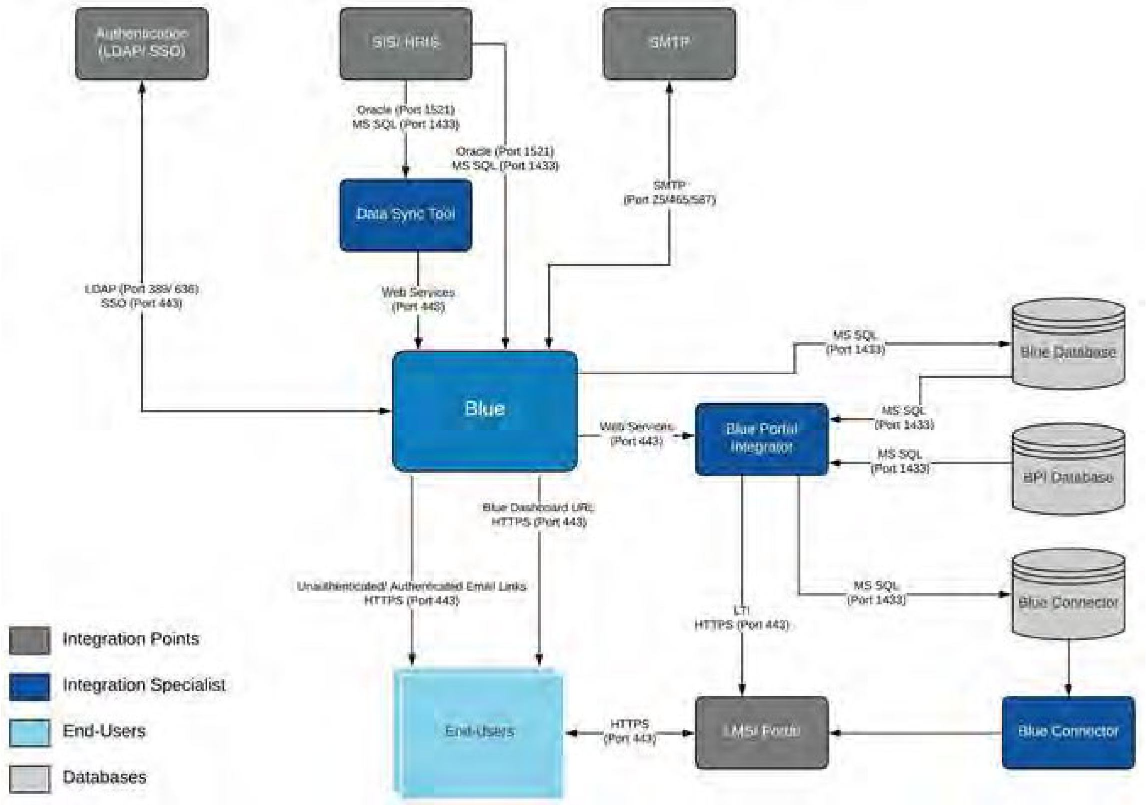

WEB
MOBILE
SCREEN READERS
Alternative input devices
VPAT
ACCESS
AUTHENTICATION
SSO (Shibboleth, CAS, Cosine, SAML)
LDAP (Active Directory)
AUTHENTICATION
REPORTING & ANALYTICS
Flexible reports
Web Services APIs:
Blackboard Analytics, IBM Cognos, Canvas Data, Moodle X-Ray, Ellucian Perform, etc.
OUTPUT
PRESCRIPTIVE ANALYTICS
blue
LEARNING ECOSYSTEM INTERACTION
SIS (Grade Pathways, Course Registration Gateway, Report Triggers, etc.)
LMS (Course Level Integration, Notifications, Calendar, Alerts and Pop-ups, etc.)
ENGAGEMENT
COLLABORATION
EVALUATION
DATA
ENGINE
METADATA
EMAIL
Deliver evaluation tasks
DATA INTEGRITY GATEWAY (DIG)
Ensure data integrity
Expand data set
Automate evaluations
Enrich analytics
INPUT
INFORMATION SYSTEM INTEGRATION
SIS (Peoplesoft, Colleague, Workday, CAMS, Calista, Banner, PowerCampus, Jenzabar)
LMS (BbLearn, Brightspace (D2L), Sakai, Canvas, Moodle)
CRM (Dynamics, Salesforce CRM)
ERP/HRIS (SAP, Oracle)
BPM (Zendesk, Workfront)
Other (Portals, social, mobile)

Figure 2: Secondary Overview of Blue's System Architecture



A summary of the data flows between ECU and Blue are described below:

1. ECU determines the unique data elements from ECU’s SIS (Colleague) that will form the relationship table for Blue, linking student and course instructor to course survey requirements.
2. ECU discloses the relationship table to Blue via Blue’s Data Sync Tool (API).
3. Blue collects the personal information in the relationship table provided by ECU and stores it in encrypted format in Blue’s ECU instance.
4. Blue uses the information to create a “task” for each student – linking the requirement for each student to complete a course evaluation to the student’s record in Blue.
5. Blue launches the task and triggers a notification to the student via email or a notification once logged into the Self-Service Portal (LMS).
    a. Where an email is triggered, ECU will use Blue’s SMPT functionalities to deliver emails via ECU’s email server.
    b. Where a notification is provided by the LMS, ECU will utilize Blue’s Blue Connector (API) to initiate pop-up box reminders that will appear once a student has logged on to the system.
6. The student clicks the survey link, which sends the student to authenticate via ECU’s LDAP system. The username used to authenticate is validated with the username provided by ECU to Blue in the SIS relationship table, providing the student with the necessary course surveys. To note, Blue does not receive or store any LDAP passwords.
7. The student completes and submits the survey. While the survey response is considered anonymous to the instructor, the student may include information that could be potentially identifiable to the instructor in any free-text boxes comments.
8. The survey responses are stored as raw data and aggregated to form summary reports. Access to raw data is determined by role-based permissions. Once submitted, the raw data (original survey responses) are stored as an encrypted file; a copy of the student’s unique data elements is also appended to the raw data file.
9. Instructors and administrators login to Blue to interact with survey responses and reports using the login access points delegated to them (same as students).
10. Instructors view final course evaluation reports which include aggregates of the students’ responses and the free text/qualitative comments. Instructors can export and print PDF copies of the aggregate reports.
11. Administrators use the reports and raw data (if a role with privileges to access raw data is provisioned) for assessing the course and its outcomes, and supporting the review of faculty contracts and related negotiation activities.

2. What is the scope of this PIA?

The following considerations are within scope of this PIA:

- The technical, administrative and physical controls presented by Blue to protect the privacy of student and instructor personal information throughout the data lifecycle;
- Blue's Canadian-based data hosting service;
- The personal information collected, used and disclosed by ECU, students, instructors and Blue in the administration of course evaluation surveys; and
- The ECU systems that will interface with Blue to support its use (LDAP, SIS, LMS), but limited to the activities and interactions with Blue.

The following considerations are outside of this PIA's scope:

- Activities and interactions of the ECU systems, including the new Self-Service LMS, that do not involve the use of Blue for the purpose of course evaluation surveys;
- Blue's Azure hosting option;
- The privacy impacts of de-commissioning OA Solutions for WebAdvisor (MyEC) web-portal;
- Potential future uses of Blue's functionalities outside of course evaluation surveys; and
- Potential future uses of the data collected by Blue and downloaded by ECU.

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

1) Specific to Students:

   a. LDAP username and password

   b. Student ID number

   c. Student's Emily Carr email address

   d. Course section number and course title (for each course enrolment)

   e. Survey responses: see Appendix B for list of questions. Students could include information in the free text boxes that could identify them

2) Specific to Course Instructors/Staff:

   a. LDAP username and password

   b. Business contact information (not considered personal information)

   c. Course section number and course title (not considered personal information)

   d. Views and opinions about the instructor (considered personal information of the instructor)

3) Audit and Monitoring Data:

   a. Audit log data - System usage information is generated/retained by Blue to assist with troubleshooting, logging, and general operation. For ECU data, logs capture:

      i. Administrator activities: login and out activity and changes by those who hold an administrator role and any logins with an "impersonator" role. Actions logged include the Admin ID, session time, changes made to projects by the Administrator and source IP address.

ii. Error logs: logs are captured for all roles, which log the unique ID of the user who had the error and the error reason. Blue will use this information to determine the error source and follow-up requirements with the user.

iii. Troubleshooting data: If requested by the ECU, Blue Customer Support may access data from the relationship table for troubleshooting purposes. All access by Blue is logged (user ID, login, logout, activities performed, source IP address).

4. Does the initiative include personal information?

Yes

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

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. They will guide you through the completion of your PIA.

Part 2 – Collection, Use and Disclosure

Fill in the first column of this table. The University Privacy Office will identify whether each step represents collection, use, or disclosure and will make sure you have legal authority for what you want to do. The Privacy Office completes the shaded section of the table. Add or delete rows as needed.

Use this column to describe the way personal information moves through the initiative step by step as if you were explaining it to someone who does not know about your initiative.	Collection, use, disclosure	FOIPPA authority	Other legal authority
Step 1: ECU discloses relationship table to Blue to set up distribution and collection of course evaluation surveys	Disclosure	33(2)(d)	N/A
Step 2: Blue uses the information in the relationship table to link course evaluation tasks to students	Use	32(a)	N/A

Step 3: Blue circulates surveys to students through the approved mechanism (email, LMS access)	Use	32(a)	N/A
Step 4: Students login via LDAP and complete the surveys and submit their responses to ECU via Blue	Collection/Use/ Disclosure	26(c); 32(a); 33(2)(d)	N/A
Step 5: Instructors login via LDAP and ECU discloses results to course instructor in Blue, which may include views and opinions about the instructor in either quantitative or qualitative formats.	Disclosure	33(2)(d)	N/A
Step 6: For the purposes of troubleshooting, users may disclose personal information to Blue to support issues encountered when using the software.	Disclosure	33(2)(t)(i)	N/A
Step 7: For the purposes of initial system installation, ECU provides Blue representatives access to systems and data to support initial system installation	Use/Disclosure	32(a); 33(2)(t)(i)	

5. Collection Notice

Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA), RSBC 1996, c.165, as amended. This information will be used for the purpose of completing standard course and instructor evaluation activities. Emily Carr University collect, uses, retains, and discloses information in accordance with FIPPA. Questions may be directed to Emily Carr University's Privacy Officer: Adrian Tees (email: adriantees@ecud.ca)

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.

6. Is any personal information stored outside of Canada?

No.

To note, any notification via email will utilize ECU's M365 services, which includes storage of Azure Active Directory data outside of Canada and is covered under the ECU M365 PIA.

7. Does the initiative involve sensitive personal information?

No

Whether or not personal information is sensitive can depend on context, including where and how the information is stored. This means that answering this question will depend on the context of the initiative. Sensitive personal information is expressly or implicitly confidential (e.g., Personal financial information, geolocation data, and Personal health information). Information about sexual orientation, gender identity, religious or political beliefs, and race or ethnicity, also are widely accepted as being "sensitive".

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

Data type	Organization	Location
Relationship table	Blue by Explorance	Blue Datacenter (iWeb's Colocation Data Centre Services), Montreal, Canada
Survey responses (raw data and aggregates)	Blue by Explorance	Blue Datacenter (iWeb's Colocation Data Centre Services), Montreal, Canada
System documentation (e.g., audit logs, troubleshooting)	Blue by Explorance	Blue Datacenter (iWeb's Colocation Data Centre Services), Montreal, Canada
Backups	Blue by Explorance	Blue Datacenter (iWeb's Colocation Data Centre Services), Montreal, Canada
Physical backups	Blue	Blue Headquarters, Montreal, Canada
User authentication (LDAP); Student Information System (SIS); Learning Management System (LMS)	ECU	ECU datacenter, Vancouver, Canada

Additional information:
Where information is stored in Blue's datacenter, the datacenter is hosted by the iWeb's Colocation Data Centre Services System located in Montreal Canada. Each institution has a fully separate database & instance of the Blue software. All data-in-transit is encrypted with a minimum of TLS 1.2 and all data-at-rest is encrypted with a minimum of AES-256. The entire Blue environment is backed up including all operating system software, utilities, security software, application software, and data files necessary for recovery. Backups are performed on a dedicated backup server according to the schedule below:

- SQL Database - full SQL database backup is performed daily to the backup server. Incremental backups are performed every s.15 [redacted]
- Application - A snapshot of the application configuration files is performed daily.

Backups are moved off site weekly and stored at Blue's Headquarters in Montreal, Canada. At Blue's Headquarters, access to backups is limited to authorized personnel only and is restricted, controlled, and monitored using electronic swipe access, biometric entry and video surveillance.

Blue retains backups for a period of four weeks before rewriting. Requests to restore data on the production environment must be made, in writing, by the primary business owner.

Part 4 – Assessment of Disclosure Outside of Canada

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You will likely need your Privacy Office's help to complete this section.

All data will be stored inside Canada; Part 4 does not need to be completed for this initiative.

9. Is the sensitive personal information stored by a service provider?

N/A

10. Describe the contractual terms in place (if applicable).

N/A

11. Are you relying on an existing contract, such as an enterprise offering from BCNet?

N/A

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

N/A

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

N/A

14. Describe the privacy risks for disclosure outside of Canada?

N/A

Part 5 – Security of Personal Information

15. Does the initiative involve digital tools, databases or information systems?

Yes

16. Do you or will you have a security assessment to help you ensure the initiative meets the reasonable security requirements?

A security assessment is currently underway by ECU. Blue has provided evidence of its validated security controls through the SOC 2 Type 2 report, and a completed Higher Education Community Vendor Assessment Toolkit (HECVAT) report. See Appendix A for an additional privacy risk assessment provided by Blue concerning collection, use, and disclosure of personal information within Blue's systems.

17. Controlling and tracking access - Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We allow employees only in certain roles access to information Role-based access determines level of access to reports and raw data for system users. Administrator: • Role to be assigned to one representative that is responsible for course evaluation across the institution • Role will have access to all surveys and reports including all raw data (Blue can configure permissions so that no roles have access to the raw data as well) • Role is responsible for appointing and setting access permissions for remaining roles Project manager: • Role can be assigned to more than one person • Role will have access to surveys and reports that they were given access to by the Administrator (often a subset of the institution that they are overseeing e.g., department/faculty) • Role may have access to raw data if access permissions are in place Subjects: • Role is assigned to individuals who are being evaluated (i.e., instructors) • Role can only access reports for each course they are teaching (no access to raw data; however, access restrictions must be configured in the system) Default users: • Role is assigned to students who are engaging in the task • Role can only access the survey they are tasked to complete (no access to report or raw data) Inactivity timeouts are set to 40 minutes by default for all roles but can be configured to suit the needs of ECU.	Yes

Employees that need standing or recurring access to personal information must be approved by the appropriate authority Blue employees: Secure access to customer information is limited to a “need-to-know” basis. Blue uses Microsoft Active Directory for both internal and external users. There are no shared accounts or local accounts used. Accounts are reviewed/audited to ensure appropriate access on a day-to-day basis. After initial installation, authorized Blue employees will only have access if requested by ECU. ECU employees: See above re role-based access; at the time of writing, ECU was in the process of developing an access matrix for Blue.	Yes
We use audit logs to see who accesses a file and when Audit log data: System usage information is generated/retained by Blue to assist with troubleshooting, logging, and general operations. For ECU data, logs capture: • Administrator activities: login and out activity and changes by those who hold an administrator role and any logins with an “impersonator” role. Actions logged include the Admin ID, session time, changes made to projects by the Administrator and source IP address. • Error logs: logs are captured for all roles, which capture the unique ID of the user who had the error and the error reason. Blue will use this information to determine the error source and follow-up requirements with the user. • Troubleshooting data: If requested by the ECU, Blue Customer Support may access data from the relationship table for troubleshooting purposes. All access by Blue is logged (user ID, login, logout, activities performed, source IP address). Login audits are stored for 12 months. System logs are stored for a minimum of 45 days. A request must be made for access to logs. All logs are encrypted at rest and transit. All logs are available upon request by the ECU. Security events business process such as process abandonment, transactions, connections, performance such as data load time and page	Yes

timeouts, and data for subsequent requests for information are also logged.	
Policies and Procedures Blue: Blue's processes relating to data privacy and security overlap with multiple related policies, procedures, and processes in accordance with regulatory and legal requirements and include the following policies and processes: • Access Control (from the information security standpoint this deals with access control for logical and physical management processes required to maintain all systems and application security in the operational environment) • Account Management (to minimize the risk of unauthorized access to critical systems and infrastructure) • Asset Management (which includes rigorous guidelines for pre - and post-contractual third-party assessment and risk management) • Change Management (requiring thorough documentation, prioritization, logging, analysis (including impact assessment), proper authorization of change, emergency change classification parameters, monitoring and testing) • Corporate Information Security (ensuring implementation of risk-based protocols for the protection of information, and assets, complying with legal and regulatory requirements, meeting industry standards and best practices) • Acceptable Use (for electronic devices and network resources to ensure proper management of the risks associated with inappropriate or unauthorized use of technology) • Information/Data Classification • Incident Management (sets requirements to enable rapid recovery in a repeatable manner that results in predictable and effective results to mitigate and manage privacy-related incidents among others). a. Blue will notify ECU of any issues or issues involved with ECU's instance as soon as possible (no timeframe committed to, but ideally within 24 hours)	Yes

• Risk Management (applies to all information resources, systems, technology and users within the Blue operating environment and all its extensions) All Blue employees are required to complete yearly security training and sign confidentiality agreements. All Blue employees with access to any of ECU's systems or data will be required to undertake and commit to ECU's standard contractual, policy/procedural and training requirements. ECU: Access to the system by ECU staff and instructors is governed by ECU's policies and procedures.	
Confidentiality Controls Within Blue, ECU can configure confidentiality controls to limit disclosure of small cell size counts and small survey response counts (e.g., responses masked if cell size is less than five; surveys not aggregated or presented if response count is less than 5). This can be limited on a survey, department, or institution-wide basis. ECU can also set up filters for surveys to control and filter out certain words or phrases. ECU can enable encryption controls to encrypt the raw data generated by each survey report. As the unique identifiers from relationship table will be attached to the report, it is recommended that this setting is turned on for all reports across the institution.	Yes
Tracking and Analytics Blue does not provide tracking and analytic software on the survey system; rather it provides the option for institutions to upload their own option or outsource to Google Analytics. No further tracking or analytics software should be initiated by ECU. ECU can determine whether IP addresses and device details will be collected from students and staff when interacting with Blue. There is an option to turn on IP tracking and the collection of device details within Blue at the project level when setting up a survey. ECU must ensure tracking of IP address and device details are not initiated for any of the surveys.	Yes

Part 6 – Accuracy, Correction + Retention

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

Yes

- Blue: Blue will not be responsible for facilitating any corrections to personal information.
- Students: Student information retrieved from ECU source systems (e.g., SIS) can be corrected/updated either by contacting student services or human resources.
- Course instructors: Where course instructors have received views and opinions about themselves from students and have encountered inaccuracies and/or inappropriate opinions, course instructors will follow standard compliant procedures as set out by their respective faculty and human resources.

19. Does your initiative use personal information to make decisions that directly affect an individual(s)?

Yes

Human resources and faculty members may use the results of the aggregate reports for contract negotiation efforts with course instructors. The use of the reports will be based off a need to know to validate information previously gathered rather than as a regular requirement. This type of use is currently in place for reports produced by the current course evaluation system.

20. Do you have a retention schedule in place related to personal information used to make decisions? 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?

At the time of writing, ECU did not have a standard records management policy in place for these types of records. The timeline from the current course evaluation system for raw data and aggregate reports is set to six years to ensure alignment with financial retention timelines. It is recommended that the current timeline is retained until an institution-wide records management policy and schedule are instated.

Where ECU terminates the contract, all data will be returned in CSV format via the method agreed upon with the institution. The ECU instance and all associated information and files will be destroyed from Blue active systems and archives including backups and off-site backups within 30 days.

Recommendations

The following recommendations were developed to mitigate risks arising from this assessment and should be implemented prior to the installation of Blue:

- **Disclosure of student's first and last name:** At the time of writing, ECU was working with Blue to determine the utility of providing student's first and last name in the relationship table (in addition to the other data elements provided). ECU must determine whether these data elements will be provided prior to the implementation of Blue and this PIA must be updated accordingly.

- **Access matrix:** ECU must develop an access matrix that outlines which categories of staff and faculty should have access to Blue's user roles. Limitation must be placed on roles that can access raw data (Administrator and Project Manager) and controls must be configured within Blue to support the implementation of the "need to know" and "least privilege" principles for each role.
- **Data retention timelines:** Apart from developing an institution-wide records management policy and retention schedule, ECU must confirm the recommendation for retention of course evaluation records as outlined in this version of the PIA.
- **Collection limitation controls:** ECU can determine whether IP addresses and device details will be collected from students and staff when interacting with Blue. There is an option to turn on IP tracking and the collection of device details within Blue at the project level when setting up a survey. ECU must ensure tracking of IP address and device details are not initiated for any of the surveys.
- **Confidentiality controls:**
  - ECU must configure confidentiality controls to limit disclosure of small cell size counts and small survey response counts (e.g., responses masked if cell size is less than five; surveys not aggregated or presented if response count is less than 5) on a per-survey basis.
  - ECU must enable encryption controls to encrypt the raw data generated by each survey report. As the unique identifiers from relationship table will be attached to the report, it is recommended that this setting is turned on for all reports across the institution.
- **Contractual controls:**
  - The current version of the master service agreement with Explorance does not consider foundational privacy controls in the body and appendices. Explorance has been provided with the FIPPA privacy protection schedule for review and integration into the next version of the contract.
  - Explorance does not commit to a specific timeframe for breach notification – ECU should require a maximum of 24 hours from time of discovery for inclusion in the next version of the contract.
  - An updated NDA should be signed by all Explorance/Blue staff that will have access to ECU's systems and/or data for the purposes of initial installation and long-term support.
- **Survey disclaimer:**
  - ECU should draft and append a survey disclaimer to all surveys that reminds student to not include any personal or sensitive information in the free text boxes.

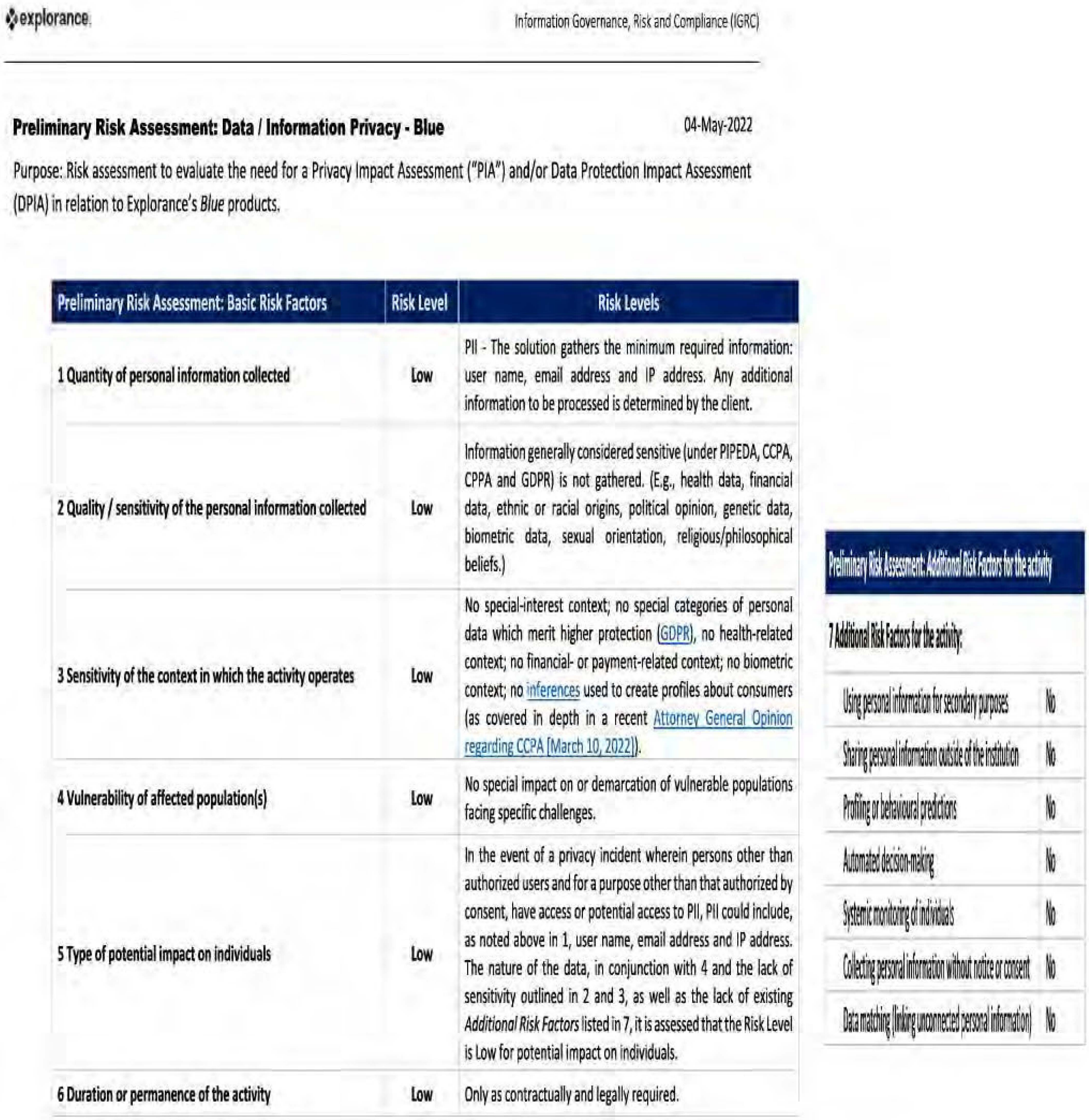
Part 7 – Program Area Signatures

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, a PIA Update must be completed and submit it to Privacy Office(r).

Ali Entezari *Department/Unit Manager*	Signature Ali Entezari	Date 14th March 2023
Sandeep Sidhu *Chief Information Officer*	Signature Sandeep	Date 14th March 2023
Adrian Tees *Privacy Officer*	Signature	Date 14th March 2023

A final copy of this PIA (with all signatures) must be delivered to privacy@ecuad.ca for record keeping.

APPENDIX A: Blue's Privacy Report Card



explorance

Information Governance, Risk and Compliance (IGRC)

Preliminary Risk Assessment: Data / Information Privacy - Blue 04-May-2022

Purpose: Risk assessment to evaluate the need for a Privacy Impact Assessment ("PIA") and/or Data Protection Impact Assessment (DPIA) in relation to Explorance's *Blue* products.

Preliminary Risk Assessment: Basic Risk Factors	Risk Level	Risk Levels
1 Quantity of personal information collected	**Low**	PII - The solution gathers the minimum required information: user name, email address and IP address. Any additional information to be processed is determined by the client.
2 Quality / sensitivity of the personal information collected	**Low**	Information generally considered sensitive (under PIPEDA, CCPA, CPPA and GDPR) is not gathered. (E.g., health data, financial data, ethnic or racial origins, political opinion, genetic data, biometric data, sexual orientation, religious/philosophical beliefs.)
3 Sensitivity of the context in which the activity operates	**Low**	No special-interest context; no special categories of personal data which merit higher protection (GDPR), no health-related context; no financial- or payment-related context; no biometric context; no inferences used to create profiles about consumers (as covered in depth in a recent Attorney General Opinion regarding CCPA [March 10, 2022]).
4 Vulnerability of affected population(s)	**Low**	No special impact on or demarcation of vulnerable populations facing specific challenges.
5 Type of potential impact on individuals	**Low**	In the event of a privacy incident wherein persons other than authorized users and for a purpose other than that authorized by consent, have access or potential access to PII, PII could include, as noted above in 1, user name, email address and IP address. The nature of the data, in conjunction with 4 and the lack of sensitivity outlined in 2 and 3, as well as the lack of existing *Additional Risk Factors* listed in 7, it is assessed that the Risk Level is Low for potential impact on individuals.
6 Duration or permanence of the activity	**Low**	Only as contractually and legally required.

Preliminary Risk Assessment: Additional Risk Factors for the activity	
7 Additional Risk Factors for the activity:	
Using personal information for secondary purposes	No
Sharing personal information outside of the institution	No
Profiling or behavioural predictions	No
Automated decision-making	No
Systemic monitoring of individuals	No
Collecting personal information without notice or consent	No
Data matching (linking unconnected personal information)	No

APPENDIX B: Current Course Evaluation Survey Questions (Still To be Confirmed)

ECU Course Evaluation Form

1. The material and discussions were relevant to the course.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

2. Sufficient time was allocated to introduce the concepts.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

3. The number of credits was sufficient to the workload.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

4. The material was presented in an organized and understandable way.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

5. The curriculum was challenging and stimulating.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

6. Overall I am satisfied with my learning and with the quality of the course.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

Instructor Evaluation

7. The Instructor stimulated my interests in this subject.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

8. The Instructor promoted an environment that helped me to learn.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

9. The Instructor encouraged class participation.
Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

10. The Instructor used class time effectively.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

11. The Instructor demonstrated current knowledge of the subject.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

12. Grading criteria were clearly described and discussed.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

13. The Instructor gave constructive feedback.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

14. The Instructor was respectful and considerate.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

15. The Instructor was accessible to students.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

Student Information

16. The group dynamic in the class was positive for learning.

Strongly Agree Agree Neutral Disagree Strongly Disagree N/A

17. On average, how much time per week do you spend preparing for this course?

1-3 hrs 4-6 hrs 7-9 hrs 10 or more hrs

Any Additional Comments