Part 1 – General Information

Name of Department/Unit	Office of the Registrar; Student Services	**Project ID**	2024-07
PIA Drafter	Kaitlyn Gutteridge		
Email	kgutteridge@ecuad.ca	**Phone**	778-833-0628
Project Sponsor	Kathryn Verkerk, Registrar, Executive Director of Enrollment		
Email	kverkerk@ecuad.ca	**Phone**	
Project Manager	Kathryn Verkerk, Registrar, Executive Director of Enrollment		
Email	kverkerk@ecuad.ca	**Phone**	

1. What is the initiative?

ECU requires a streamlined and sustainable process for verifying the legitimacy of international student documents and credentials during the admission process for undergraduate programs. This type of review is critical under the new Immigration, Refugees and Citizenship Canada (IRCC) legislation, which considers modifications to the International Student Program (ISP).

To date, review of international students' credentials and documentation has been completely internally by Admissions staff; however, no defined process or training have been in place within ECU to guide this work.

The Registrar's Office has received approval to engage with a Canadian service provider, International Credential Assessment Service of Canada (ICAS), to complete the review process. The benefits of outsourcing to ICAS include:

- Builds integrity into admission processes by verifying the legitimacy of international student documents and credentials (critical under the new IRCC legislation).
- Improves the student experience for international applicants as they will receive an admission decision from ECU quicker.
- Increases time for recruiters to focus on yield conversion of international admits (critical to ECU's income requirement).
- Ensures students satisfy ECU's Senate mandated admission requirements (i.e. minimum required academic courses and GPA).
- Saves hiring additional admissions staff to manage complex international evaluations.
- Saves training admissions staff annually on international credential verification.
- Shifts the focus for admissions to review domestic applications.

ICAS is a Canadian company with over 20 years of experience in the assessment of international credentials. Their review of documentation and reports generated support employers, education institutions, immigration officials and community agencies understand the education international applicants have completed outside Canada.
ICAS is a member of the Alliance of Credential Evaluation Services of Canada, and is designated by the Minister of Immigration, Refugees and Citizenship to provide assessments for individuals who are applying

for immigration to Canada. ICAS is an approved provider of credential assessment services for individuals applying to colleges in Ontario through ontariocolleges.ca (Ontario College Application Service/OCAS).

ECU and ICAS have developed a process and determined the appropriate infrastructure requirements to complete the review of international students' documentation and credentials. The process and infrastructure are described herein.

Process Overview

ECU collects applications and supporting documentation from international students using the same approach in place for domestic students, which is further described in the SlideRoom PIA (PIA# 2024-08).

Upon receipt of the documentation, ECU will transfer the transcripts of international students (PDF version) to a secure folder on the ECU Admission's OneDrive (more information about infrastructure requirements below). ECU will also include an Excel file in the OneDrive folder that includes the first and last name of the student and their ECU application reference number (one student per row). This Excel template has been created by ICAS and will be used to document ICAS' findings from their review of the documentation. The Excel document will be generated by ECU and completed by ICAS for each "batch" of transcripts that ECU provides to ICAS for review.

Once the transcripts and Excel file are stored in the OneDrive folder, authorized ICAS staff members (approximately two) will login to ECU's SharePoint site to review the transcripts and complete their review of the credentials described in each transcript. All findings and feedback reported by ICAS will be saved within the Excel file. ICAS will send notice to ECU's Registrar by email once their review and report are complete.

Where ICAS requires additional information or notes questions for follow-up in the Excel file, authorized staff from ECU's Admission's office will follow-up with ICAS by documenting the requested information in the Excel file. Upon resolution of any outstanding items, ICAS will certify the completion of the Excel file and the Excel file will become the official report for all transcripts reviewed within the batch provided to ICAS by ECU.

ICAS will download a copy of the report and securely retain the file for one year for tracking and monitoring purposes, as well as to fulfill accounting requirements.

ECU will consult the final report provided in the Excel file to:

- Determine the legitimacy of each international students' credentials;
- Assess the students' alignment with ECU's mandated admissions requirements, and
- Make decisions about admissions acceptance for international students.

Once the batch of transcripts and Excel file have been used by ECU to make their decisions about the students' admissions eligibility, ECU Admissions will move the transcripts and Excel file to a separate folder within the Admissions OneDrive to limit ICAS' reoccurring access to the transcripts post-completion of their review. This clean-up process will permit for the folder to be re-used for the next batch without creating and adjusting folder permissions for each new batch.

This process will be completed routinely at a regular cadence for all new application intake openings starting February 2025.

Infrastructure Overview
ECU IT will create a new shared folder within ECU Admission's OneDrive. Within the folder, ECU will set up permissions for ECU Admissions / Registrar's Office to have read and write access to the documentation. It will also set up a generic ECU M365 account (email address and internal network access) for ICAS.

The ICAS account will be created in accordance with ECU's policies and procedures, including M365 Terms and Conditions. The ICAS account permissions will be strictly limited to accessing the ICAS folder set up on the Admission's OneDrive and will not have any other access granted (email, other ECU systems or folders etc.). The ICAS account will have read and write permissions for the ICAS folder only.

ICAS will routinely send a list of authorized individuals with access to the ECU ICAS account for ECU to hold on file.

Prior to providing ICAS access to the ECU account, ECU IT will complete all testing activities required to certify account permissions are appropriately configured.

2. What is the scope of this PIA?

- Use of ICAS for the review and assessment of international students' credentials for undergraduate programs.
- Use of ECU's internal M365 infrastructure to host the documentation and provide access to ICAS for review.

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

Transcript
Given the diversity of educational institutions and non-conformity of requirements for information elements provided in the transcripts, a wide range of information may be presented in the transcript. This includes:

- Student's first and last name
- Student's date of birth
- Student's father's first and last name
- Name of student's educational institution
- Student number for the corresponding educational institution
- Address of the educational institution
- Name of the principal for the educational institution
- Passport Number or a similar country-specific identification number
- Name of courses completed at the educational institution, year, and corresponding grades

ICAS Excel File Reporting Template
The following information will be recorded in the Excel file for each student / transcript assessed:

- ECU application reference number
- First and last name

- Country
- Assessment type
- Outcome 1
- English studies
- 2 Academic
- 2 Additional Academic or Elective
- GPA
- Note (any questions / further feedback from ICAS)

4. Does the initiative include personal information?
Yes – please see list above.

Part 2 – Collection, Use and Disclosure

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	Personal Information
1. ECU collects international students' applications and supporting documentation including transcripts upon submission of an application for ECU admission.	Collection	26(c)	Yes
2. ECU Admission's staff create a batch of transcripts and complete the ICAS Excel template, and transfer the files to the shared ECU OneDrive folder.	Use	32(a)	Yes
3. ICAS accesses the OneDrive folder and completes their review of the transcripts and produces a final report (Excel file) that describes their assessment of the international students' credentials.	Use	32(a)	Yes

4. ECU uses the findings outlined by ICAS in the Excel file to make decisions about students' eligibility for admissions	Use	32(a)	Yes
5. ICAS downloads a copy of the completed Excel file to retain for one year for the purposes of monitoring and reporting, and accounting.	Use; Retention; Storage	32(a); 30; 31	Yes
6. ECU retains the Excel file in accordance with ECU records retention requirements. Given the information is used to make a decision about an individual, it must be retained for at least one year.	Use; Retention; Storage	32(a); 30; 31	Yes

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

5. Collection Notice

No additional collection notice is required for the collection of personal information considered in this initiative. A collection notice is already provided to students upon submission of their application, which covers this type of assessment by ECU for the purpose of adjudicating applications and making admissions decisions.

Part 3– Storing Personal Information

6. Is any personal information stored outside of Canada?

No personal information will be stored outside of Canada. The personal information will be stored in a OneDrive folder within ECU's M365 instance, which is hosted in Canada. ECU's M365 license has been previously assessed by ECU; please refer to the M365 PIA for additional information about the physical and technical infrastructure.

The completed Excel file is downloaded and stored by ICAS for one year within ICAS' local secure infrastructure that is wholly hosted on premise within ICAS' offices in Guelph, Ontario, Canada. Need to know and least privilege access is applied to the Excel file, which is limited to ICAS staff within the Management and Accounting Department.

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

Please see question 6 above.

8. **Does the initiative involve sensitive personal information? If yes, where and how are you storing the personal information involved in the initiative?**

   No sensitive personal information is involved in this initiative.

Part 4 – Assessment of Disclosure Outside of Canada

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. Otherwise continue to Part 5.

Part 4 is not applicable to this PIA – please see additional information in Part 5.

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

If yes, fill in the table below (add more rows if necessary)

Name of service provider		

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

If you wish to modify the Privacy Protection Schedule, email privacy@ecuad.ca

Describe the contract details including duration

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

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

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

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

Part 5 – Security of Personal Information

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

Yes, it involves ECU's M365 instance, which has been previously assessed by ECU (see M365 PIA).

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

Yes, a security assessment has been previously completed for M365.

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	Yes / No and please describe
We allow employees only in certain roles access to information ECU Access to the transcripts, shared folder on OneDrive and Excel file will be limited to Admissions' staff with a need to know. ECU's Registrar will communicate these requirements (and any subsequent changes) to ECU IT who will oversee set-up and maintenance of the folder. ICAS ECU IT will create a new shared folder within ECU Admission's OneDrive. Within the folder, ECU will set up permissions for ECU Admissions / Registrar's Office to have read and write access to the documentation. It will also set up a generic ECU M365 account (email address and internal network access) for ICAS. The ICAS account will be created in accordance with ECU's policies and procedures, including M365 Terms and Conditions. The ICAS account permissions will be strictly limited to accessing the ICAS folder set up on the Admission's OneDrive and will not have any other access granted (email, other ECU systems or folders etc.). The ICAS account will have read and write	Yes

permissions for the ICAS folder only. ICAS will routinely send a list of authorized individuals with access to the ECU ICAS account for ECU to hold on file. Prior to providing ICAS access to the ECU account, ECU IT will complete all testing activities required to certify account permissions are appropriately configured. ICAS staff must complete ICAS' privacy and security training yearly.	
Employees that need standing or recurring access to personal information must be approved by the appropriate authority Please see description above.	Yes
We use audit logs to see who accesses a file and when Standard ECU M365 logging and monitoring requirements will be configured by ECU IT for the shared folder. Auditing of logs will be completed by ECU IT in accordance with ECU's policies and processes.	Yes
Additional strategies: <u>Time-imposed limits on access to transcripts</u> Once the batch of transcripts and Excel file have been used by ECU to make their decisions about the students' admissions eligibility, ECU Admissions will move the transcripts and Excel file to a separate folder within the Admissions OneDrive to limit ICAS' reoccurring access to the transcripts post-completion of their review. This clean-up process will permit for the folder to be re-used for the next batch without creating and adjusting folder permissions for each new batch.	Yes

Part 6 – Accuracy, Correction + Retention

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

Any international student who seeks access, or who seeks to correct, amend, or delete their own inaccurate data, must direct the query to ECU. Standard ECU procedures for requests to correct or amend information will apply upon receipt of a request.

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

Yes, personal information submitted by the international student will be used to make a decision about the student's admissions status (approve or deny).

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?

Yes, ECU Admissions has a process in place for retaining personal information collected from internationals students (please see SlideRoom PIA for additional details about initial collection of transcripts).

ICAS will retain Excel files for one year for reporting / monitoring / accounting purposes, after which they will be securely destroyed from ICAS local network and back-ups.

Part 7 – Additional Risks

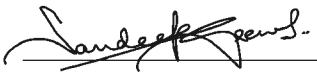
In the table below describe any additional risks that arise from collecting, using, disclosing, or storing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Response
Risk 1: ECU will be entering into a MOU with ICAS for the provision of ICAS' services. No FIPPA compliance privacy schedule has been introduced into the MOU. As a service provider to ECU, ICAS must agree to comply with FIPPA and adopt obligations outlined in the FIPPA privacy schedule.	FIPPA privacy schedule to be included as an appendix to the MOU and signed off by ICAS. Kaitlyn Gutteridge to draft privacy schedule for inclusion in the MOU.

Please ensure Parts 7 and 8 are attached to your submitted PIA.

Part 8 – Program Area Signatures

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

Department Manager	Signature	Date
Sandeep Sidhu		16 Dec 2024
Sandeep Sidhu *Chief Information Officer*	Signature	Date
Adrian Tees *Privacy Officer*	Signature	Date

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

APPENDIX A – SUPPLEMENTARY AI ASSESSMENT

OVERVIEW

1. Is AI technology used in this initiative (whether standalone technology or integrated into a larger offering)?

   No – no further responses to questions in Appendix A required.

2. Type of AI technology that will be used (select all that apply):
   - ☐ Machine Learning: learns patterns from data, e.g., email automation and spam filtering
   - ☐ Deep Learning: intricate pattern recognition, e.g., automated cars
   - ☐ Generative AI: creates new content, e.g., ChatGPT
   - ☐ Natural Language Processing: language recognition and processing, e.g., spellcheck
   - ☐ Other
3. What is the purpose/function of the AI technology (select all that apply):
   - ☐ Prediction modelling
   - ☐ Other record abstraction
   - ☐ Chatbots
   - ☐ Social media sentiment analysis
   - ☐ Translation or Speech-to-text
   - ☐ Image recognition - identifiable images
   - ☐ Image recognition - non-identifiable images
   - ☐ Image classification
   - ☐ Object detection
   - ☐ Voice recognition
   - ☐ Automation
   - ☐ Other:
4. How will the AI technology be used (select all that apply)?
   - ☐ Existing AI technology will be used to generate or collect data
   - ☐ Existing AI technology will be evaluated/will be the focus of this work
   - ☐ New AI technology will be created and validated
   - ☐ New AI technology will be created, validated and used to generate or collect data
5. Who created the AI technology and why was it selected? Is the AI developed in-house by the vendor or supplied by a third party?

DATA

6. What type of information will be inputted into to the AI technology (select all that apply)?
   - ☐ Directly identifying information
   - ☐ Indirectly identifying information
   - ☐ Non-identifiable data
   - ☐ Identifiable images/videos
   - ☐ Non-identifiable images/videos
   - ☐ Audio

- ☐ Biometric data
- ☐ Location data
- ☐ IP address
- ☐ Web tracking data
- ☐ Other

7. Will the input data be retained by the AI technology (e.g., for future re-training)? Y/N
8. Will the use of the AI technology generate any new identifiable information (output data)?
    a. If so, what type of information will be generated?
        - ☐ Directly identifying information
        - ☐ Indirectly identifying information
        - ☐ Non-identifiable data
        - ☐ Identifiable images/videos
        - ☐ Non-identifiable images/videos
        - ☐ Audio
        - ☐ Biometric data
        - ☐ Location data
        - ☐ IP address
        - ☐ Web tracking data
        - ☐ Other

9. Provide an overview and technical documentation of the AI infrastructure and data flows.
10. Where will the data be stored? Where will the log files, backups and other transitory files be stored?
11. How long is the data, log files, back-ups, and transitory files retained and how is it securely disposed of when no longer needed? What controls are in place to ensure data is not used beyond its original purpose?
12. How will the data be de-identified or anonymized? Is there any risk of de-anonymization?
13. What controls are in place to limit who has access to input and output data, and all other files (log, back-up, transitory etc.)? Describe the access controls and authentication processes in place.
14. What audit controls are in place to capture trails of how the data and files are moved and stored from one location to another during the information lifecycle.
    a. How does the vendor ensure that data or files are not misused by those who have access?
    b. Who has access to the data or files and under what conditions (including third-parties)?
15. Is the AI technology auditable from ECU's endpoint? Can ECU customize the audit process?
16. What agreements are in place between the vendor and ECU? Is a privacy protection schedule included?
17. How does the vendor respond to privacy incidents or breaches? Is there a robust incident response plan in place?

AI TECHNOLOGY

18. How has the AI technology been validated?
19. Is the AI technology being used for its intended purpose?
20. Is the AI technology locked or adaptive?
    a. Adaptive (learns in real-time)
    b. Locked (does not change over time)

21. What are the broad kinds of algorithms that will be used to create models from the data?
22. What are the features that may be used in each model?
23. What are the key model parameters?
24. What justifications, if any, have the vendor provided for the assumptions, boundaries, and limitations of the AI model?
25. What is the target output of each component of the model (what is being predicted or classified); how did the vendor determine whether the output of each component is suitable for the operational context?
26. To what extent are the outputs consistent with the vendor's values and principles to foster public trust and equity?
27. What are the key evaluation metrics and loss functions, such as the trade-off between false positives and false negatives; what justification is used for the metric selection? Who is responsible for developing the metrics? To what extent are the metrics consistent with the vendor's goals, objectives, constraints (including ethical and compliance considerations)?
28. What monitoring processes are in place to monitor model performance drifts, and model activities?
29. What biases, inequities, and other societal concerns have been identified as potential risks resulting from the AI technology? What procedures are in place to mitigate these risks?
30. Describe the plan to control for AI technology bias in the results.

SECURITY

31. Assess and document the security risks of the AI technology. How is data protected during transmission? Does the vendor use encryption protocols like Transport Layer Security (TLS) to protect data in transit?
32. Does the vendor have third-party security certifications (like ISO 27001, SOC2, etc.) that verify their security posture? How regularly are these certifications reviewed and renewed?
33. How does the vendor protect against vulnerabilities in the AI, including adversarial attacks? What is the patch management policy and how quickly are vulnerabilities resolved?
34. How does the vendor respond to security/cybersecurity incidents? Is there a robust incident response plan in place?
35. Is there a possibility of the AI making uncontrolled, unsupervised decisions that could impact security?

TRAINING

36. How will the AI technology be trained in advance of use and will it require ECU data? If so, what type of data will be inputted?
    a. Document the data collected to train the AI technology and assess its identifiability, whether it is accurate, adequate, relevant, and limited to the purpose(s).
37. What external data sources were used to train the AI technology? How or from whom was the data obtained? To what extent is the vendor relying on scraping publicly available data from the Internet to train model(s) and from which websites?
38. What controls are in place to limit who has access to training data, training code, and deployment code.
39. How will the training data be de-identified or anonymized? Is there any risk of de-anonymization?
40. What audit controls are in place to capture trails of how personal data is moved and stored from one location to another during the training and testing phase. How does the vendor ensure that data isn't misused by those who have access? Who has access to the data and under what conditions? Are there strong access controls and authentication processes in place?

FIPPA ACCESS, CORRECTION, DECISION MAKING

41. How transparent is the AI technology's decision-making process?
42. Will any decisions be made about a person based on the AI technology? If so, how will they be validated?
43. Assess and document the explainability of the AI technology and consider what supplementary tools that can used to help explain decisions made by the AI technology to individuals who will be affected.
44. Document how ECU will facilitate individual rights requests throughout the lifecycle of the AI technology where personal information will be processed.