Privacy Impact Assessment

PIA# 23-001

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:	**Exam Soft Software (for Faculty of Law exams)**		
Name of TRU Department/Branch:	Faculty of Law		
PIA Drafter (you):	Lana Walker		
Your Email:	lawalker@tru.ca	Phone:	250.852.7268
Service/Vendor:	**Kevin Stringfellow**		
Vendor Email:	**kstringfellow@examsoft.com**	Phone:	**214-720-6126**

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

Privacy Impact Assessment

PIA# 23-001

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.

This proposed change gives TRU the opportunity to provide a better service to its law students, while simultaneously relieving some of the demand on TRU's IT Services' time capacity required in monitoring law exams. Exam Soft provides more, and more direct, service with its software than the software currently used for law exams (Exam4). s.13 [redacted]

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.

This PIA covers the ExamSoft project as a replacement for Exam4. It will cover the data sources that ExamSoft may use and the specific data fields within that data source. A HECVAT assessment of their service is included as in-scope to ensure ExamSoft is providing adequate security to protect this information. The use and protection of this data is covered under FOIPPA regulation.

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

Yearly license

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 – no previous PIA.

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.

The complete list of elements and instructions to upload are available here: Legacy Portal: Import Exam Takers & Courses, and Create Exam Taker Groups (examsoft.com).

Specifically, 3 files are necessary:

1. **List of courses: 7 fields:**
    a. Course ID: Unique identifier for the course
    b. Course name: Name for the course
    c. Instructor LName: Instructor last name
    d. Instructor Fname: Instructor first name
    e. Instructor Title: (Optional) Dr., Ms., Mrs., Mr., etc.
    f. Start Date: Date when the course is available
    g. End Date: Date when the course is closed

2. **List of students: 6 fields:**
    a. ExamTakerID: A unique alphanumeric ID (with no special characters or spaces) to identify this exam-taker. (*This would be the TID of the student).*
    b. Fname: The exam-taker's first name.
    c. Lname: The exam-taker's last name.
    d. Email: The exam-taker's email address.
    e. Passwd: A password consisting of six to 12 alphanumeric characters (with no special characters or spaces). *(not needed. ExamSoft can use TRU single-sign-on).*
    f. LabEquip: A setting that is used to identify exam-takers who are using shared devices in a lab; none of their personal data is stored on the lab device.
    g. Accommodation Group #: The rule number for any accommodation rule(s) that apply to this exam-taker

3. **Course/Student relational list: 2 fields**
    a. ExamTakerID: A valid ExamTaker ID *(imported from list-of-students CSV)*
    b. ExamNum: A number assigned to an exam *(previously entered in ExamSoft Portal)*

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)?

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

Examsoft uses a managed service provider, LightEdge, located in Austin, TX and Kansas City, MO, ss their infrastructure-as-a-service(IaaS) hosting solution. Description of their security services is available here: https://www.lightedge.com/compliance-security. LightEdge has undergone SSAE-18 audit and SOC2/SOC3 compliant.

6. Common or Integrated Program or Activity (required)

If you answer yes, please contact the *Privacy and Access Officer*

If you answer "yes" to all 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.	

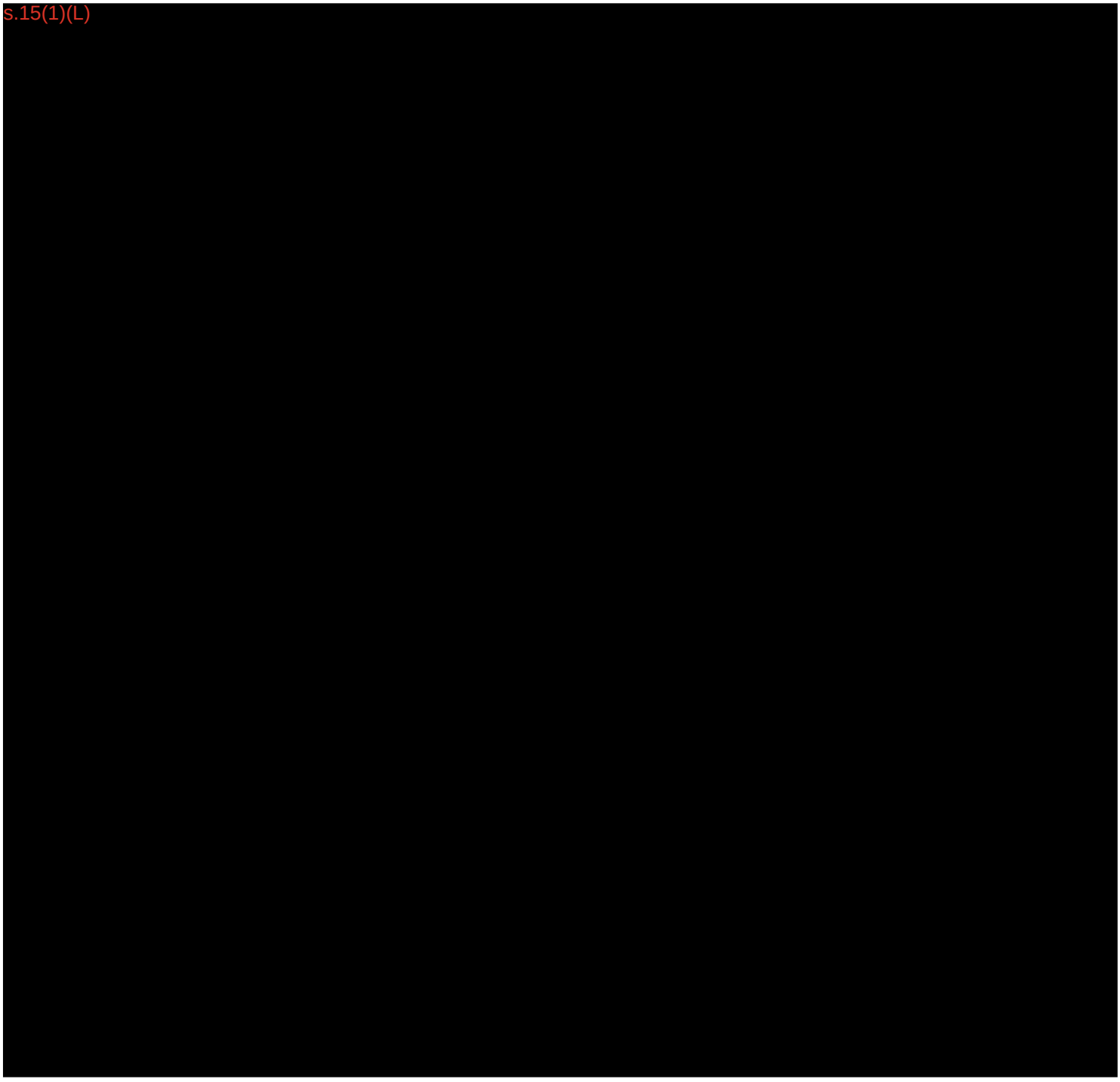
7. Data-linking Initiative* (required)

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;	no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	n/a
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.	n/a

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.

s.15(1)(L)



Personal Information Flow Table.

Personal Information Flow Table			
Step	**Description/Purpose**	**Type**	**FOIPPA Authority**
1.	IT Enterprise Systems uploads data (see part I. Q4) via secure protocol.	Disclosure	33(2)(d)
2.	IT Client Services downloads and installs Examplify APP on lab computers.	N/A	N/A
3.	TRU Law Professor logs into ExamSoft Portal via TRU SSO	Use	32(a)
4.	Professor creates law exam with answer key.	N/A	N/A
5.	TRU Law Student logs in. Downloads exam via Examplify APP installed on TRU desktop.	Use	32(a)
6.	Proctor gives student password to unlock the exam	N/A	N/A
7	Internet access disabled. Student takes exam offline	N/A	N/A
8.	Student completes exam. Internet access enabled. Exam uploaded to ExamSoft servers for auto marking. Downloaded exam in step 5 deleted from desktop computer.	Collection and Use	26(c), 32(a)
9.	Professor logs into ExamSoft Portal to review exam scores.	Use	32(a)

Risk Exposure Matrix ***(for question 9 below)***

Risk Exposure Matrix			**IMPACT**			
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
LIKELIHOOD	**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

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented.

Risk Mitigation Table

Step	Risk	Mitigation Strategy	Likelihood	Impact	Exposure
1.	s.13	[redacted]			
2.					
3.					
4.					
5,6,7					
8.					

9.	s.13 [redacted]

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

s.13 [redacted].

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.

Collection Notice Statement - Template

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 administer exams for the Faculty of Law department through a 3rd party service provider ExamSoft. ExamSoft collects any information that you provide in the process of registering a user account with, subscribing to ExamSoft's services and/or email notifications, or using ExamSoft's software to take or mark an exam. Specifically:

- your name
- student/employee number,
- email address,
- exam answers, and other assessment content.

For questions about how your personal information is being collected, please contact *Lana Walker (lawalker@tru.ca), Assistant Dean, Faculty of Law*.

Further information can be found on ExamSoft's privacy policy at: https://examsoft.com/privacy-policy.

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.

See HECVAT: (DATA-20), (DATA-21), (DATA-22), (PHYS-02), (PHYS-03), (PHYS-04), (PHYS-05), (DCTR-15), (DCTR-16), IaaS provider is SOC 2/3 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.

See HECVAT: (DOCU-01), (DOCU-04), (DOCU-06), (COMP-05), (APPL-05), (APPL-06), (APPL-11), (APPL-17), (DATA-01), (DATA-02), (DATA-03), (DATA-04), (DATA-06), (DATA-15), (DATA-16), (DATA-17), (DATA-18), (DATA-19), (DATA-20), (DATA-21), (DATA-22), (DATA-26), (DBAS-01), (DBAS-02), (DCTR-14), (DRPL-05), (DRPL-06), (DRPL-10), (FIDP-02), (FIDP-05), (FIDP-09), (FIDP-10), (MAPP-05), (MAPP-06), (MAPP-07), (MAPP-010), (SYST-03), (VULN-01), (VULN-02), (VULN-03), (VULN-04), (VULN-05), (VULN-08)

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.

Yes, see HECVAT: (QUAL-04), (QUAL-05), (DOCU-06), (CHNG-01), (CHNG-08), (CHNG-12), (CHNG-13), (CHNG-15), (DATA-23), (DATA-25), (PPPR-02), (PPPR-07), (PPPR-09), (PPPR-10), (PPPR-13), (PPPR-16), (PPPR-17), (PPPR-19), (SYST-02), (SYST-04), (THRD-01), (THRD-02), (THRD-03), (THRD-04).

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.

See HECVAT: (APPL-01), (APPL-02), (APPL-11), (APPL-15), (APPL-16), (AAAI-01), (AAAI-02), (AAAI-03), (AAAI-04), (AAAI-09), (AAAI-10), (AAAI-12), (AAAI-17),(CHNG-01), (DATA-01), (DATA-16), (DATA-25), (DATA-26), (DCTR-03), (DCTR-09)

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.

See HECVAT: (APPL-15), (APPL-16), (AAAI-15), (AAAI-16), (DATA-17), (DATA-22), (DCTR-09), (PHYS-01), (PHYS-02), (PHYS-05), (PPPR-19)

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.

The courses CSV file, and the students CSV file is uploaded by TRU. Latest upload of information overwrites the previous data so changes and accuracy of data is controlled by TRU.

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

No. The system simply marks exams created by the instructor and uploaded to our service using the instructor's provided answer key.

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.

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.

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. **NO**

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. **NO**

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. **NO**

23. Does this initiative involve the disclosure of personal information that is sensitive to be stored outside of Canada?

The initiative involves disclosure of information to be stored in in Austin, TX and Kansas City, MO. While the use of ExamSoft does not necessariy entail the provision of sensitive PI, there is some chance sensitive information could be disclosed as part of the examination process.
This PIA has therefore addressed the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining:

a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;

b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;

c. whether the personal information is stored by a service provider; and,

d. where the personal information is stored.

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

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

25. 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])?

(1) to notify its users and customers of any issues affecting ExamSoft's services and software, and the resolution thereof. (2) marketing or other promotional communications.

26. 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?

Use "unsubscribe" or "opt-out" link at the bottom of such emails, or contact ExamSoft directly.

27. 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**)..

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

[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.

Part 8a – Information Security Director Comments

s.13 [redacted]

John Cuzzola	s.22 [redacted]	2023-02-23
Information Security Director	Signature	Date

Part 8b – Privacy Officer Comments

s.13, s.14 [redacted]

Marina Sparks	s.22 [redacted]	March 6 2023
Privacy and Access Officer	Signature	Date

Part 9 – Program Area Signatures

Program/Department Manager John Cuzzola	Signature s.22 [redacted]	Date 2023-02-23
Information Security Director	Signature	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).***