

Privacy Impact Assessment

PIA# 25-0007

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).

Please note: Depending on the dollar amount or length of the agreement you intend to enter into with a third party, you may need to engage the Procurement Services Department. Please see the TRU Purchasing Policy (BRD 02-2) for more information.

Initiative Preamble (Required)

Initiative/ Project/ Program Name:	BitRecover MSG to PDF Wizard		
Name of TRU Department/Branch:	Privacy and Access Office		
PIA Drafter (you):	Marina Sparks, Privacy and Access Officer		
Your Email:	msparks@tru.ca	Phone:	778-694-2424
Service/Vendor:	BitRecover		

Privacy Impact Assessment

PIA# 25-0007

Vendor Email:	support@bitrecover.com , sales@bitrecover.com	Phone:	1 616 314 5060
---------------	--	--------	----------------

Have you consulted IT Department for this Initiative/Project/Program?

Yes X No N/A

(If no, it is recommended to consult IT Department first to resolve any potential IT-related issues.)

Part 1 – General

1. Description of the Initiative (required)

BitRecover MSG to PDF Wizard is a MSG to PDF converter that allows you to batch convert MSG files (Outlook emails) to PDF. It lets you convert large batches of MSG files (including attachments) to PDF and provides options for formatting file names, including an option to rename files by date.

In the course of processing access to information applications, the privacy office will often receive many emails that must be manually converted to PDF so that redactions can be applied and other security features may be used. Currently, attachments must also be converted separately and attached to the corresponding email, which is incredibly time consuming/inefficient.

BitRecover will allow the Privacy Office to quickly and easily convert the entire batch of emails responsive to an access application in a way that ensures all files are accounted for and organized properly.

The software is purchased and downloaded online, and is used entirely offline; BitRecover will not have access to any information processed using the software, nor will any other third party.

This software is currently in use at UBC and VIU.

2. Scope of this PIA (required)

This PIA covers the use of the BitRecover MSG to PDF Converter Wizard for use by the Privacy and Access Office to convert emails that have been gathered in response to an access to information application.

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

This is a one time purchase.

3. Related Privacy Impact Assessments

None.

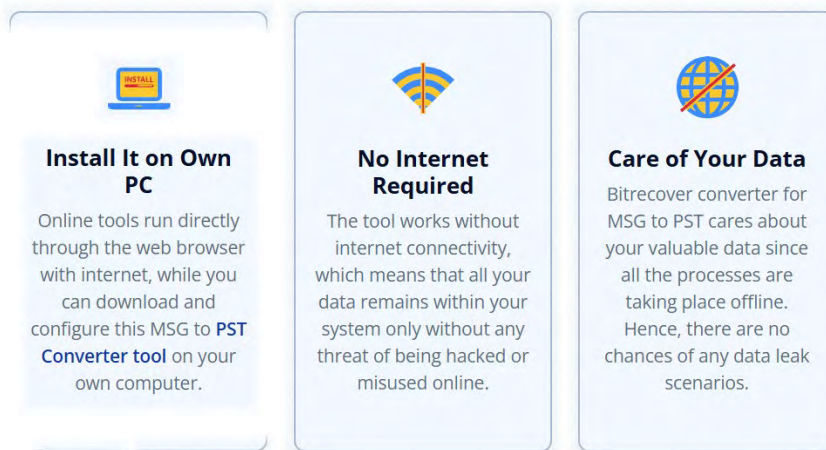
4. Elements of Information or Data (required)

BitRecover will only be given access to the personal information involved in purchasing the software and communicating with BitRecover about the software/use of their services, per their privacy policy

- Billing, shipping and contact information necessary to complete purchase.
- Contact information (name and email address) for communicating with help center.
- Name and email will also be used to send BitRecover newsletter, which can be opted out of.

Privacy Policy: <https://www.bitrecover.com/privacy-policy.html>

The records involved in processing an access application may contain any kind of personal information, including sensitive personal information, however the tool works offline and no third party access is granted to records processed using BitRecover. Their website confirms the tool works offline, and all data remains within TRU systems:



<https://www.bitrecover.com/msg-to-pst/>

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada (required)

Files processed using BitRecover will remain on TRU systems.

Privacy Impact Assessment

PIA# 25-0007

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

No, we are not contracting with BitRecover (except to the extent we agree to their T&Cs when purchasing the software), it is a one time purchase.

6. Common or Integrated Program or Activity (required)

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

If you answer “yes” to <u>all</u> 3 of these questions, your initiative qualifies as “a common or integrated program or activity,” and you must comply with requirements under FOIPPA.	
1. This initiative involves a program or activity that provides a service (or services);	yes/ no
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;	yes/ no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/ 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.	yes/ no

Privacy Impact Assessment

PIA# 25-0007

7. Data-linking Initiative* (required)

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

If you answer “yes” to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under FOIPPA.	
1. Personal information from one database is linked or combined with personal information from another database;	yes/no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes/no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	yes/no

8. Provide a diagram, flowchart, and/or table that shows how your initiative will collect, use, and/or disclose personal information.

Personal Information Flow Table			
	Description/Purpose	Type	FIPPA Authority
1.	Information is gathered from within TRU in response to an access to information application	Disclosure	s.33(3) – enactment of BC that requires the disclosure, the enactment being FIPPA. S.33(2)(h) – necessary for Privacy Officer to perform their employment duties.
2	Where records provided in response to access application include of Outlook MSG files, BitRecover may be used to convert these to PDF for further processing.	Use	s.33(2)(c), the applicable s.33 subsection

Privacy Impact Assessment

PIA# 25-0007

			being s.33(2)(e) and s.33(2)(h).
3			
4			

9. Risk Mitigation Table (required)

Please identify any privacy risks associated with the initiative and the mitigation strategies that will be implemented. Please identify the likelihood (rare, unlikely, possible, likely, almost certain) and the degree of impact (insignificant, minor, moderate, major, catastrophic).

Risk Mitigation Table					
	Risk	Mitigation Strategy	Likelihood	Impact	Exposure
1	s.13				
2					
3	Risk:				

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

Risk Exposure Matrix

Privacy Impact Assessment

PIA# 25-0007

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

10. Collection Notice

Emails processed using BitRecover will have been gathered by the Privacy and Access Office in the course of completing internal searches in response to access to information applications. This is information that is already in the custody or control of the University, and those asked to provide the records will be advised of the legal basis for our seeking them.

Part 3 – Security of Personal Information

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

N/A, PI is not accessed by third parties.

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

N/A, PI is not accessed by third parties.

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

N/A, PI is not accessed by third parties.

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)

s.13, s.14

Privacy Impact Assessment

PIA# 25-0007

s.13, s.14

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

TRU is purchasing the BitRecover MSG to PDF Wizard that can be used by 5 accounts. Records collected/processed in the course of responding to access applications will be only accessed by those who have a need to access this information as part of their employment duties. The information will be stored in secure folders on the (O:) Drive, which is only accessible to those who require this as part of their role.

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.

TRU's use of BitRecover will not involve collecting new personal information, this does not apply.

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

No.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate, complete and up-to-date.

N/A

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

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.**

Privacy Impact Assessment

PIA# 25-0007

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

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.

No

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

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

No

24. If you answered yes to question 23, please explain the purpose(s) of the messages you intend to send. Be sure to note any messages involving promotional activities, including links to the TRU public website or other Internet site(s). The purpose(s) you provide will help us identify whether the overall communication is a commercial electronic message (CEM¹)?

N/A

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

N/A

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

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

N/A

Part 7 – Common Vulnerabilities and Exposures (CVE) Assessment

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

This initiative does not involve the transmission of personal data between TRU and the vendor – contact information given to BitRecover should only be business contact information.

Privacy Impact Assessment

PIA# 25-0007

Part 8a – Information Security Director Comments

John Cuzzola

s.22 [Redacted Signature]

2025-02-27

Information Security Director

Signature

Date

Part 8b – Privacy Officer Comments

Marina Sparks

s.22 [Redacted Signature]

27-02-2025

Privacy and Access Officer

Signature

Date

Part 9 – Program Area Signatures

Privacy Impact Assessment

PIA# 25-0007

Program/Department Manager	Signature	Date
John Cuzzola		2025-02-27
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).***