COLLEGE OF THE ROCKIES

Privacy Impact Assessment Form

Name of Initiative: HALO ITSM
PIA Number: N/A

INSTRUCTIONS (READ BEFORE STARTING)

Submit a completed privacy impact assessment (PIA) before starting a new College Initiative or significantly changing an existing College Initiative that directly collects Personal Information, or results in the collection of Personal Information by COTR or a COTR service provider.

BC's Freedom of Information and Protection of Privacy Act (FIPPA) defines an "Initiative" as any enactment ("policy/procedure"), system (conceptual or technical), project, program, or activity.

Contact the COTR Privacy Officer (PrivacyOfficer@cotr.bc.ca) to receive support determining whether any change in how COTR employees are completing their duties to the College may require a Privacy Impact Assessment.

Read through this form entirely before starting to populate it. Each question is designed to capture specific information for review.

Some information recorded in the PIA may be confidential or proprietary and not intended for distribution. Before you share the draft or completed PIA (internally or externally), please contact COTR'S Privacy Officer at PrivacyOfficer@cotr.bc.ca for guidance.

PART 1: GENERAL INFORMATION

Initiative Title:	Halo ITSM
Department:	Technical
Initiative Lead (PIA Drafter) Name and COTR Email Address:	Kyle Brown kbrown@cotr.bc.ca
Executive Leadership Team member sponsor	Nathan Skretting, VP Strategy, Budget & Operations nskretting@cotr.bc.ca
Privacy Officer Name and Email Address::	

Is this an Initial PIA or an update (include previous PIA #)	☒Initial ☐ Update Previous PIA #:

1. **Describe the initiative in enough detail that a reader who knows nothing about your work will understand what the implementation of the initiative will accomplish and how it will operate within your business. 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.**

   The more sensitive the personal information used in the initiative, for example health care information, the more fulsome this description and the analysis below should be.

   The IT Department is deploying a new, unified service platform called Halo ITSM; this platform will replace several other services at the College (such as Smartsheet and potentially FAME for Facilities use).

S. 17(1)(c)

2. **Will the initiative include the use of 3rd party software that will be installed within our network or accessed via a cloud service?**

   ☒ **Yes** ☐ **No**

   If yes, document the vendor and the software to be used.

Third Party Name:	Halo
Product Name (if applicable):	Halo ITSM

Third Party Contact Name and Email:	Reid Benson Reid.benson@imaginehalo.com
Third Party URL:	https://usehalo.com/haloitsm/
Third Party address of headquarters	Halo House, Gipping Way Stowmarket United Kingdom
Will the software be installed on our network	No
Will the software be accessed in the cloud?	Yes
Will data be stored in Canada or outside of Canada?	In Canada

3. **Scope of this PIA: Will this initiative be part of a larger initiative or rolled out in phases?**

☐ **Yes** ☒ **No**

If yes, what part of the larger initiative does this PIA cover, and if relevant, what will it not cover?

S. 17(1)(c) [redacted]

4. **Information inventory: List the elements of information or data that will be collected, used, disclosed, and retained in relation to the initiative.**

S. 17(1)(c) [redacted]

[redacted]

5. **Did you list Personal Information in question 4? 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.**

☒ **Yes** ☐ **No**

6. **If you answered "No" to question 5, explain how you will ensure that you do not unintentionally collect personal information?**

S. 17 (1)(c) [redacted]

7. **If you answered "No" to question 5, you do not need to complete the rest of this form.**

PART 2: COLLECTION, USE AND DISCLOSURE

8. ***Acquiring consent: Note how you will acquire consent from individuals. For example, will the consent be written, verbal, or implicit? If verbal, how will you record the consent? If implicit, how is the collection obvious to a reasonable person. If you are collecting the personal information from another organization, document how you will obtain sufficient information to determine that they collected the personal information with consent and that you are only using the personal information for the purpose(s) they gave the individual.***

   The consent is implicit as the individual will be entering their own data for the purpose of completing the ticket.

9. **Authority for collection, use and disclosure: For each data element identified in section 4 that is personal information, use the table below to document the legal authority to collect, use or disclose the information.**

Data element	FOIPPA authority to collect, use or disclose	Other legal authority to collect, use or disclose
[redacted]	Section 28 of FOIPPA	
	Section 28 of FOIPPA	
	Section 28 of FOIPPA	
	Section 28 of FOIPPA	
	Section 28 of FOIPPA	
	Section 28 of FOIPPA	

S. 15(1)(l), s. 17(1) and s. 19(1)

10. **Collection, use and disclosure notice: If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice. The collection notice must contain at a minimum:**
    - **The purpose of the collection, use or disclosure**
    - **Legal authority to collect, use or disclose the information, and**
    - **Who to contact for more information about the collection, use or disclosure of personal information.**

    Example: ***The College of the Rockies ("COTR") collects your Personal Information in accordance with section 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA"), for the purposes of providing administrative support. If you have any questions about the processing of your Personal Information, please contact the privacy officer at privacyofficer@cotr.bc.ca.***

    Document your notice for collection, use or disclosure below:

    The College of the Rockies ("COTR") collects your Personal Information in accordance with section 26 of the Freedom of Information and Protection of Privacy Act ("FIPPA"), for the purposes of providing administrative support. If you have any questions about the processing of your Personal Information, please contact the privacy officer at privacyofficer@cotr.bc.ca.

11. **Withdrawing consent: Consider the implications of an individual withdrawing their consent for the collection, use, and disclosure of their personal information. Consider implications for how the individuals information will be removed from the initiative.**

    N/A

PART 3: STORAGE

12. Is all Personal Information involved in your Initiative stored within standard COTR storage locations, technologies, or services?

[redacted] S. 15(1)(l), s. 17(1) and s. 19(1) [redacted] S. 15(1)(l), s. 17(1) and s. 19(1)

13. If you answered No to question 18, where is the geographical location of where the personal information is stored? Please identify applicable geographic locations for primary storage and backups. Please note every primary and back-up storage if there is more than one.

Primary Storage	Back-up Storage (if applicable)
[redacted]	

S. 15(1)(l), s. 17(1) and s. 19(1)

14. Is any personal information involved in your Initiative stored outside of Canada?

☐ Yes ☒ No

15. Is any of the personal information being stored outside of Canada sensitive personal information? This would be any information classified as M or H in section 4.

☐ Yes ☒ No

If Yes, complete Part 4. If No, go to Part 5

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section only if you answered Yes to Section 15 and you will be storing sensitive personal information outside of Canada.

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

☐ **Yes** ☒ **No**

If yes, complete the table below.

Company name of service provider	Application or platform name	Where is the sensitive personal information stored (including backups)

17. **Is the information being disclosed to third parties outside of Canada to other than the service providers listed in section 16?**

☐ **Yes** ☒ **No**

18. **If you answered Yes in section 17, to whom will the information be disclosed and for what purpose?**

Entity to whom the information will be disclosed	Purpose for disclosure	Where is the sensitive personal information stored (including backups)

19. **If you answered yes in section 16 or 17, do you have a contract with the third party that includes privacy-related terms?**

☐ **Yes** ☒ **No**

Attach a copy of the contract to the PIA.

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

21. Provide details of how you will track access to sensitive personal information. What logging and monitoring will be in place?

22. Describe the privacy risks for disclosure of sensitive personal information outside of Canada.

Privacy Risk	Impact to individual	Likelihood of unauthorized collection, use disclosure or storage of sensitive personal information (H/M/L)	Level of privacy risk (L/M/H) considering the impact and likelihood	Risk response	Residual risk

The outcome of Part 3 will be a risk-based decision by the President of the College of the Rockies, as head of a public body, on whether to proceed with the initiative and share sensitive personal information outside of Canada.

PART 5: INFORMATION FLOW

23. Complete the Information Flow Table

Use column 1 to describe the way Personal Information moves through your Initiative step by step. Describe the steps as if you were explaining it to someone who does not know about your Initiative.

Use column 2 to identify whether the action in column 1 is a collection, use, or disclosure of Personal Information.

S. 17(1)(c)

Information Management Steps	Collection, use, or disclosure	FIPPA and other legal authorities	Identify if there are COTR or 3rd party controls in place to protect the collection use and disclosure of personal information
[redacted]			

S. 17(1)(c)

[redacted]

Insert a drawing or flow diagram here or in an appendix to explain the interconnection of all of the parts of the system and how the data flows through the system for collection, use and disclosure of personal information.

S. 17(1)(c)

[redacted]

PART 6: SECURITY OF PERSONAL INFORMATION

How will the initiative secure personal information to protect privacy. People, organizations, or governments outside of your Initiative should not be able to access the Personal Information you collect, use, store or disclose. You need to make sure that the Personal Information is safely secured in both physical and technical environments.

24. **What administrative safeguards are in place to protect Personal Information?**

If any Administrative safeguards were identified in the Information Flow Table, describe the source of the safeguards and the details of the safeguards in the tables below that protect where the records for your Initiative are stored.

S. 15(1)(l), s. 17(1) and s. 19(1)

What is the documented source of the safeguards at COTR and the Third Party:

Safeguard	Name of Document
[redacted]	

Safeguard	At COTR	At Third Party
[redacted]		

S. 15(1)(l), s. 17(1) and s. 19(1)

S. 15(1)(l), s. 17(1) and s. 19(1)

[redacted]

25. If any Technical safeguards were identified in the Information Flow Table, describe the source of the safeguards and the details of the safeguards in the tables below that protect the records in transit and where the records for your Initiative are stored.

Describe the elements of technical security that protect where the records for your Initiative are stored (e.g. secure passwords, encryption, firewalls, etc.) (More options on the following page)

What is the documented source of the safeguards at COTR and the Third Party:

Safeguard	Name of Document
[redacted]	

S. 15(1)(l), s. 17(1) and s. 19(1)

Safeguard	At COTR	At Third Party
[redacted]		

S. 15(1)(l), s. 17(1) and s. 19(1)

[redacted]

26. **If any Physical safeguards were identified in the Information Flow Table, describe the source of the safeguards and the details of the safeguards in the tables below that protect where the records for your Initiative are stored.**

What is the documented source of the safeguards at COTR and the Third Party:

Safeguard	Name of Document
[redacted]	

S. 15(1)(l), s. 17(1) and s. 19(1)

Safeguard	At COTR	At Third Party
[redacted]		

S. 15(1)(l), s. 17(1) and s. 19(1)

If the Initiative involves a Third Party, please indicate what type of Agreement governs the relationship between COTR and the Third Party. Please select all that apply and attach as an appendix to the PIA.

[redacted]

S. 15(1)(l), s. 17(1) and s. 19(1)

[redacted]

S. 15(1)(l), s. 17(1) and s. 19(1)

27. **What is the documented source of the Privacy related terms at the Third Party:**

Document name	Privacy related sections
Halo Privacy Policy	https://usehalo.com/privacy-policy

PART 7: ACCURACY AND CORRECTION

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's Personal Information is accurate and complete. FIPPA also gives an individual the right to request correction of errors or omissions to their Personal Information.

Is there a reasonable risk that if inaccurate information is entered into the system/initiative, use of that information could cause harm to an individual? Will decisions be made based on the personal information that will directly affect the individual?

For example, If an individual's date of birth is an important criterion in determining eligibility for a benefit, any appropriate supporting documents such as birth or baptismal certificates should be reviewed.

☐ **Yes** ☒ **No**

If Yes, complete this section. If No, continue to the next section.

In this section, please demonstrate how you will make a reasonable effort to ensure the Personal Information you have on file is accurate and complete.

28. **How will COTR ensure that the Personal Information is accurate and complete? (Check all that apply)**

- ☐ Individuals input their own Personal Information
- ☐ Individuals update their own Personal Information
- ☐ Employee verifies that information is accurate and complete before processing
- ☐ Documented processes to ensure accurate and complete data entry and maintenance
- ☐ The Third Party manages the accuracy and completeness of Personal Information under the direction of COTR
- ☐ Software or service uses automated processes to enter and manage Personal Information
- ☐ Other: (*fill in details*)
- ☐ Other: (*fill in details*)

29. **Is there a documented process in place to correct Personal Information?**

Document name	Relevant sections

30. **Sometimes it is not possible to correct the Personal Information. FIPPA requires a process to make a note on the record about the request for correction if it isn't possible to correct the record itself. Is there a documented process in place to annotate the record?**

☐ **Yes** ☐ **No** ☒ **N/A (Corrections possible)**

Document name	Relevant sections

31. **If there is a request for correction from an individual and COTR or the Third Party disclosed that individual's Personal Information in the last year, FIPPA requires that COTR or the Third Party provide the applicable other public body or Third Party about the request for correction. Will COTR or the Third Party ensure that these notifications are done when necessary?**

- ☐ COTR will forward correction notifications
- ☐ Third Party will forward correction notifications
- ☐ COTR and Third Party will split responsibility based on who was authorized to disclose Personal Information to third parties before a correction request was made.

PART 8: RETENTION AND DISPOSITION

FIPPA requires that public bodies keep Personal Information for a minimum of one year after it is used to make a decision. Personal Information needs to be disposed of to limit privacy risk after legal retention timelines.

32. **Is COTR responsible for destroying records at the end of the retention period?**

[redacted] **Yes** S. 17(c) [redacted] **No** S. 17(c)

If Yes, complete question 33. If No, complete question 34.

33. **How long will COTR need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.**

Record Type	Retention Period (Years/Months)	Notes:
[redacted]		

S. 17(c)

34. **Is the Third Party responsible for destroying records at the end of the retention period?**

[redacted] **Yes** S. 17(c) [redacted] **No** S. 17(c)

If Yes, complete section 35. If No, continue to section 36.

35. **How long will the Third Party need to retain the records containing Personal Information? If there are different retention timelines for different types of records, please state each retention timeline based on record type.**

S. 17(c) [redacted]

S. 17(c)

Record Type	Retention Period (Years/Months)	Notes:
[redacted]		

36. **How will you ensure that the records containing Personal Information are disposed of in accordance with the retention schedule noted in questions above? (Check all that apply)**

[redacted]

S. 17(c)

Document name	Relevant sections
To be finalized later (6-12 months) – In active process of building out procedure document.	TBA

37. **What methods will be used to dispose of Personal Information following retention period? (Check all that apply.)**

S. 17(c)

[redacted]

S. 17(c)

[redacted]

PART 9: TRAINING

38. **Identify which of the following activities all employees and Third Party (as applicable), will be trained on when collecting and managing the Personal Information for the College Initiative.**

- ☒ Collection: Limit the collection to only what is explicitly necessary
- ☒ Use: Use the Personal Information only for the purpose for which it was originally collected
- ☒ Access: Only authorized employees (and, where applicable, service providers) may access the Personal Information
- ☒ Disclosure: Not to disclose the Personal Information inside or outside COTR unless authorized under FIPPA
- ☒ Storage: To store the Personal Information only in COTR-provided or approved storage locations and not to store unnecessarily in multiple locations
- ☒ Retention: to keep the Personal Information for a minimum of one year – with longer retention periods only when necessary
- ☒ Disposal: To dispose, when applicable, in a secure method that renders the Personal Information permanently irretrievable

Provide details on when and how the training will be provided to all employees and Third Parties (as applicable):

Training	Additional details
User/Staff training will be provided by IT department on the new system, and will include a "Do/Don't" component for data entry.	To be developed as part of the initiative roll-out.
IT staff will be trained on additional elements for personal information identification and disposal where necessary/appropriate.	

PART 10: PERSONAL INFORMATION BANKS

39. **Will your Initiative result in a Personal Information Bank ("PIB")? A PIB is a collection of Personal Information searchable by name or unique identifier. If yes, please complete the table below. If more than one PIB will result, copy and paste an additional copy of the table below and fill out a separate table for each PIB.**

☐ **Yes** ☒ **No**

If Yes, complete the following table. If No, proceed to the next section.

Title	
Location	
Personal Information Types	
Categories of Individuals Included	
Collection Authority	
Purpose of Personal Information	
Categories of Persons Managing Information	

PART II: APPROVAL SIGNATURES

Institution Signatures

This PIA is compliont with FIPPA when it occurately documents information management practices and information flow at the time of signing. If there are any changes to the overall Initiative, including to the way Personal Information is collected, used, stored, or disclosed, the Department will inform the COTR Privacy Officer, and if necessary complete a PIA update.

By signing where required below, the signatories acknowledge and confirm their declarations as noted.

Declaration of Initiative Lead: I confirm that I understand the privacy impacts of this College Initiative and I am committed to my FIPPA obligations related to the collection and management of Personal Information involved in the Initiative. If there are any changes to the Initiative, including to the way Personal Information is collected, used, stored, or disclosed, I understand that the department will need to inform the COTR Privacy Officer and if necessary, complete a PIA update. I will establish and document information management guidelines for the Personal Information and ensure these are followed. I will ensure emplayees are trained on and able to comply with their obligations under FIPPA; related College policies and procedures; and COTR Privacy Officer recommendations relative to this Initiative.

Signature of Initiative Lead or PIA Drafter S. 22(1)

Name and Title	Signature	Date signed
Kyle Brown	[redacted]	Nov 14, 2025

Declaration of Dean / Director / One-Over-One Signatory: I confirm that I have reviewed this PIA and I acknowledge the residuol privacy risks identified. I support the department by providing required time and operatianal resources to comply with FIPPA, related College palicies and procedures, and COTR Privacy Officer recammendations relative to this Initiative.

Signature of Dean / Director / One-Over-One Signatory

Name and Title	Signature	Date signed
Rene Pelletier		

Declaration of Information Security: I confirm that I am satisfied that the Information Security safeguards employed in this college Initiative meet reasonable requirements relative to the amount or sensitivity of the Personal Information or COTR business information described in this PIA.

Signature of Chief Information Officer or **IT Manager** (Required only when college Initiative involves Information Security considerations)

Name and Title	Signature	Date signed

Declaration of Chief Information Officer: I confirm that I understand and approve of the proposed use-case of COTR IT systems described in this PIA, where applicable. I understand and approve of the Third Party's integration with COTR's IT systems for the College Initiative described in this PIA, where applicable.

Declaration of Head of Public Body or Designate: I hove reviewed this PIA carefully and accept and will be accountable for the residual privacy risks identified for this College Initiative. I am satisfied with the completion of this PIA under FIPPA.

PART 11: PRIVACY OFFICE(R) COMMENTS

If, in the future, any substantive changes are made to the scope of this PIA, the College will have to complete a PIA Update and submit it to Privacy Office(r).

This PIA is based on a review of the material provided to the COTR Privacy Office(r) as of **November 14th, 2025**

The details provided in this PIA, indicates that the application to be developed and uploaded onto

the COTR website can be delivered in compliance with FIPPA legislation.

Should there be a change in scope to this part of the initiative, further assessment and/or a PIA update may be required as new related or expanded service is considered, or the privacy policies for the College change in the future.

Any substantive changes made to the scope of this PIA would need to be included in a PIA update and submitted to the Privacy Office(r).

- https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00
- https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_03#section26

Privacy Office Signature

This PIA is based on a review of the material provided to the Privacy Officer as at the date in Part 13 Privacy Officer Comments above.

Name and Title	Signature	Date signed

Signature of Head of Public Body or Designate Under FIPPA (Required only if Personal Information is involved in the Initiative as indicated in Question 7).

Name and Title	Signature	Date signed
I _____ (President Name) approve proceeding with the initiative and sharing sensitive personal information outside of Canada.		