

## PART 1: GENERAL INFORMATION

|                                                 |                                                                                                           |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Initiative Title:</b>                        | eRez Life Student Housing Management Software                                                             |
| <b>Department:</b>                              | Housing Operations                                                                                        |
| <b>Initiative Lead, Name and email Address:</b> | Evan Hilchey, Interim Associate VP Admin,<br><a href="mailto:hilcheye@camosun.ca">hilcheye@camosun.ca</a> |
| <b>Privacy Officer Assigned:</b>                | Ann Behennah, <a href="mailto:privacy@camosun.ca">privacy@camosun.ca</a>                                  |
| <b>If initiative involves a vendor provide</b>  |                                                                                                           |
| <b>Vendor Name:</b>                             | eRezLife                                                                                                  |
| <b>Product Name (if applicable):</b>            | eRez                                                                                                      |
| <b>Vendor Contact Name and Email:</b>           | Kevin Caputo<br><a href="mailto:Kevin.caputo@erezlife.com">Kevin.caputo@erezlife.com</a>                  |
| <b>Vendor URL:</b>                              | <a href="http://www.erezlife.com">www.erezlife.com</a>                                                    |

### Executive Summary:

We were provided the following supporting documents by eRez Life ("eRez"):

- Architecture diagram [attached to Appendix 1 of this PIA];
- eRezLife-HECVAT [Solution Provider Response – Privacy]
  - eRez has completed an SOC2 audit for Security and Confidential Trust Services; it does not include the Privacy Trust Service Principle.
  - eRez conforms with the principles of the NIST Privacy Framework
  - the employee onboarding and offboarding policy includes training of employees on information security and data privacy.
  - eRez does not share sensitive data with third parties beyond their infrastructure environment on Amazon Web Services (AWS)
- Amazon Web Services – System and Organization Controls 3 (SOC 3 Report) – April 1 – Sept 30, 2021.
- eRez Attestation Report for SOC 2 Type 2 [Controls relevant to Security and Confidentiality Trust Services] – July 8, 2024 – January 8, 2025
- eRez Policies:
  - Policy 09 – Physical Security Policy
  - Policy 10 – Risk Management Framework
  - Policy 16 – Incident Response Plans
  - Policy 18 – Disaster Recovery Plan
  - Policy 20 – Change Management Policy
  - Policy 22 – Compliance Policy
- Information Security Policy

### Vendor Commentary:

- AWS is the only sub-processor with access to data as that is where the data is hosted;
- All Camosun data will be hosted in Canada; and
- The incident response documentation is provided within Policy 16 and 18.

## SECURITY & INTEGRATIONS

- eRezLife can provide a full HECVAT, SOC2 Type 2 Attestation, and VPAT upon request by the institution



s. 15(1)(l), 21

Ellucian Colleague integration — eRezLife is "verified for SaaS Solution" status with both Colleague and Banner, indicating compatibility and official support

### Associate Director, ITS Security Commentary:

Camosun Associate Director, ITS Security indicated that after reviewing the materials from eRez Life, he is not aware of any security concerns. He has highlighted some of the answers from their HECVAT for awareness and project planning (rather than as a security concern):

s. 15(1)(l), 21

| Question                                                                                                                       | Y/N | Comment from eRez                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Does the system have password complexity or length limitations and/or restrictions?*                                           | Yes |                                                                                                                                                                                                                                                                                                                                                                                                          |
| Will the institution's data be available within the system for a period of time at the completion of this contract?*           | Yes | All data is expunged within 30 days of contract termination.                                                                                                                                                                                                                                                                                                                                             |
| Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?* | Yes | Backups remain in the country where they are created, but backups are replicated to multiple availability zones for durability. Data is segmented from other users and accounts.                                                                                                                                                                                                                         |
| Do the contracts in place with third parties address liability in the event of a data breach?*                                 | No  |                                                                                                                                                                                                                                                                                                                                                                                                          |
| Do clients have the option to not participate in or postpone an upgrade to a new release?                                      | No  | We have a beta and production version of our application, which we manage internally. Beta is for final validation of fully stable changes, and clients cannot choose to be included or excluded from beta. Beyond this we do not maintain multiple versions of our application. All clients run on the same code, and changes are thoroughly validated across multiple configurations prior to release. |

|                                                                                                                                |     |                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?* | Yes | Backups remain in the country where they are created, but backups are replicated to multiple availability zones for durability. Data is segmented from other users and accounts. |
|--------------------------------------------------------------------------------------------------------------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Privacy Office Commentary:**

Based upon the Information as presented and understood at the time of writing, there are no major concerns with respect to eRez Life Student Housing Management Software.

## **PART 1: OVERVIEW**

1. Describe the initiative including:
  - a) what you are doing,
  - b) an overview of the process,
  - c) who is involved,
  - d) and when and/or how long your initiative runs.

The Camosun College Lansdowne Student Housing Project (CC LSHP) requires housing management software and eRez Life Student Housing Management Software ("eRez") is being considered.

ERez provides cloud-based housing and residence life management software for higher education institutions, designed for managing student housing and residence life operations in higher education institutions. It handles sensitive personal data such as student names, contact details, housing assignments and other records such as incident reports and room condition reports. It handles everything related to the student as an occupant and their housing needs (no grades or courses).

Please see Student Housing Operations Software Project Charter for additional information.

2. In a few sentences, explain the scope of this PIA. For example, is this initiative limited to specific individuals or departments at Camosun College? Is this PIA covering the full initiative or just one phase of a larger project? Are there exceptions to how the initiative will be implemented?

This PIA is limited to analysis of eRez software.

3. Is this an administrative/operational, teaching and learning, or a research initiative? Select all that apply.

☒ Administrative/Operational

4. Has a PIA previously been completed for this initiative?

☐ Yes

☒ No

☐ Not sure

5. What activities will occur within the initiative? Use the bullet points below to make action statements. Replace the example action statement. Add or delete bullets as necessary.

Data collection is used for:

- Housing applications.
  - Managing housing assignments and residence life activities.
  - Facilitating communication between students and staff.
  - Staff scheduling.
  - Supporting administrative workflows.
  - Ensuring compliance with Institutional policies.
  - Conduct and incident reporting.
6. In a bulleted list, please list all the types of data or information you might collect, use, store, disclose, or access in your initiative - even if they are not Personal Information. Replace the bullet points below with the actual elements of information or data.
- Student first and last name
  - Student ID number
  - Email and physical address
  - Phone number
  - Gender identity
  - Interaction logs (e.g. incident reports, room condition reports)
7. Did you list Personal Information in question 6? [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
8. If you answered "No" to question 7, in three to five sentences explain how will you ensure that you do not unintentionally collect Personal Information?
9. Does the initiative involve integration between Camosun College IT systems and Third-Party systems?
- ☒ Yes ☐ No ☐ N/A

If yes, list below: (put N/A on the first row if you answered No or N/A above. Add or delete rows)

Camosun IT system:

Third party system integrated: Colleague

If there is Personal Information involved in this initiative, continue to complete the remaining sections of the PIA. If there is not any Personal Information involved in this initiative, please submit questions 1-9 to the Privacy Officer along with the completed signatures page.

## PART 2: COLLECTION

FIPPA sets out rules for public bodies and their employees to collect of Personal Information. Unauthorized collection is prohibited. This section will help you identify the legal authority for **collecting** Personal Information and confirm that all Personal Information elements collected are necessary for the purpose of the initiative.

10. Whose Personal Information is collected in this initiative? Check all that apply.

- |                                                          |                                                       |
|----------------------------------------------------------|-------------------------------------------------------|
| <input checked="" type="checkbox"/> Students             | <input type="checkbox"/> Former employees             |
| <input checked="" type="checkbox"/> Prospective students | <input type="checkbox"/> Service provider employees   |
| <input type="checkbox"/> Former students                 | <input type="checkbox"/> Donors or other constituents |
| <input type="checkbox"/> Alumni                          | <input type="checkbox"/> Volunteers                   |
| <input checked="" type="checkbox"/> Employees            | <input type="checkbox"/> Other community members      |
| <input checked="" type="checkbox"/> Other _____          |                                                       |

11. How frequently will the initiative collect Personal Information?

- ☐ Single instance of collection within one semester or quarter
- ☐ Ongoing collection up to a single year
- ☒ Ongoing collection over more than one year
- ☐ Other \_\_\_\_\_

12. How many individuals' Personal Information will be collected?

- ☐ 1 - 50                      ☐ 51 - 500                      ☒ Over 500

13. If the initiative involves a Third Party, are you able to test the product to see what personal information it collects?

- ☒ Yes                      ☐ No                      ☐ N/A (No Third-Party product involved)

14. For what purpose will the Personal Information be used? (check all that apply)

- ☒ It is necessary and directly related to college operations (student housing)
- ☒ It is necessary and related to requirements stated in college bylaws, policy, and procedure.
- ☐ It is collected because collection is required or authorized under local, provincial, or federal law. Be prepared to directly cite the section of a particular law that applies if asked.
- ☐ It is collected for determining suitability for an honour or award including a scholarship, prize, or bursary.
- ☐ It is being collected for a quality assurance or improvement initiative that has been approved by the college Executive.

15. How will you reduce the risk of collecting unnecessary Personal Information? (Check all that apply.)

- ☒ The initiative will only collect specific information deemed necessary for and directly related to the initiative
- ☒ The initiative will use forms with primarily closed-ended questions and minimal open-ended questions
- ☒ The initiative will use forms with drop-down menus
- ☒ The initiative will have documented data gathering and aggregation processes for open ended submissions or fields
- ☐ The Department needs Privacy Officer review and support because none of the above apply

16. FIPPA Collection Notice: When collecting Personal Information, FIPPA requires that you provide a collection notice (except in limited circumstances). Please fill in the template collection notice below and remove bold and square brackets.

When students apply for student housing, student housing operations will provide the student with the standard collection notice in accordance with Camosun College practices.

### PART 3: USE

FIPPA sets out requirements and restrictions related to use of Personal Information. This section will help you identify the legal authority for **using** Personal Information and ensure that the use of Personal Information is limited to the original purpose for collection.

17. What is the intended use of the Personal Information collected? (check all that apply)

- ☒ The Personal Information will be used for the purposes checked off in Question 14
- ☐ The Personal Information will be used for secondary purposes, and I have a consent notice attached as an appendix to this PIA that meets the requirements found in FIPPA regulations. I will work with the Privacy Office to determine if secondary use is appropriate and compliant with FIPPA.
- ☐ The Personal Information will be used for a purpose for which the information may be disclosed to the public body under [section 33](#). The Privacy Office will attach the relevant section number to this selection if it applies.

18. How will you ensure that parties using the Personal Information will use it only for the purposes stated in 17 above? Check all that apply.

- ☒ Documented department information management practices and training
- ☒ Documented use restrictions communicated from your department to another Camosun College department
- ☒ Written contract between Camosun College and a Third Party including explicit conditions – we need to discuss the restricted access pertaining to cloud-systems. We do not want the vendor to access student personal information, and as such we will need to ensure these terms are satisfied prior to executing the contract.
- ☐ The Department needs Privacy Officer review and support because none of the above apply

19. Does your initiative use Personal Information to make decisions that directly affect an individual?
- ☒ Yes ☐ No
20. What is the intended impact of the decisions that are being made that directly affect an individual? (check all that apply).
- ☐ Directly affects academic status or grades
  - ☒ Directly affects how an individual accesses their courses, campus activities, or student supports
  - ☐ Directly affects employment status, employee remuneration, or contract opportunities, and pay
  - ☐ Directly affects how employees and service providers will complete their work
  - ☐ Directly affects how employees access campus activities and support services
  - ☒ Directly affects the College's capacity to protect individuals from harm
  - ☒ Directly affects the College's capacity to interact with and support external parties
  - ☐ Other – may affect the student residents.

#### **PART 4: STORAGE**

21. Is all Personal Information involved in your initiative stored within standard Camosun College storage locations, technologies, or services?
- ☒ Yes ☐ No

**Camosun College storage:** Please list the approved standard Camosun College storage locations, technologies and/or services.

- ☐ Microsoft 365 (SharePoint, OneDrive, Teams)
- ☒ Colleague
- ☐ D2L
- ☐ Team Dynamix
- ☐ Other: \_\_\_\_\_

#### **Local Servers (and/or Systems):**

- ☒ Vendor's Local Storage Option – please specify: Amazon Web Services – all Camosun data hosted in Canada
- ☐ Camosun College's Networked Drives
- ☐ Physical Media

#### **Cloud Hosting:**

- ☒ Vendor's Cloud Storage Option – please specify: AWS Canada: ca-central-1 and ca-west-1

22. Is any Personal Information involved in your initiative stored outside of Canada?

☐ Yes ☒ No

23. Where is the Personal Information stored? Please identify applicable geographic locations for primary storage and backups. If Personal Information is stored in more than one primary location, the Privacy Office can expand the response field in this question.

| Name of Third Party        | Name of cloud infrastructure and/or platform provider(s)<br>[Vendor's Cloud Storage Option] | Where is the Sensitive Personal Information stored (including backups)? |
|----------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Amazon Web Services Canada | Canada: ca-central-1(Montreal) and ca-west-1 (Calgary)                                      | Canada                                                                  |

24. Does your initiative involve Sensitive Personal Information? (Any Personal Information can be Sensitive Personal Information in different contexts. Please contact the Privacy Office to discuss.)

☒ Yes – potentially ☐ No

25. Is any of the Sensitive Personal Information stored outside of Canada?

☐ Yes ☒ No

26. Where is the Sensitive Personal Information stored? Please identify applicable geographic locations for primary storage and backups. **Type N/A in the cells on the first row if Sensitive Personal Information is not stored outside of Canada as indicated in Question 26.**

| Name of Third Party        | Name of cloud infrastructure and/or platform provider(s)<br>[Vendor's Cloud Storage Option] | Where is the Sensitive Personal Information stored (including backups)? |
|----------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Amazon Web Services Canada | Canada: ca-central-1(Montreal) and ca-west-1 (Calgary)                                      | Canada                                                                  |
|                            |                                                                                             |                                                                         |
|                            |                                                                                             |                                                                         |

## PART 5: DISCLOSURE

FIPPA sets out requirements and restrictions related to disclosure of Personal Information. This section will help identify the legal authority for **disclosing** Personal Information, and consider risks related to that disclosure. **Fill out this section if Question 26 was answered "Yes"**

N/A

Complete this section if you are disclosing Sensitive Personal Information to be stored outside of Canada. You may need help from the Privacy Office.

- 27.** Is any Personal Information being disclosed outside of Canada under FIPPA section 33(2)(f)? This section allows for information to be made available to the public under an enactment that authorizes or requires the information to be made public.
- ☐ Yes ☒ No
- 28.** Is any of the Personal Information being disclosed outside of Canada under FIPPA section 33(2)(p)? This section allows disclosure for the purposes of (i) a payment to be made to or by Camosun College, (ii) authorizing, administering, processing, verifying, or cancelling a payment, or (iii) resolving an issue regarding a payment.
- ☐ Yes ☒ No
- ☐ The payment processor is out of scope of this PIA
- 29.** Describe the privacy risks for disclosure of Personal Information outside of Canada.

**Use the table to indicate the privacy risks. For each privacy risk you identify, describe the potential impact to individuals or Camosun College, and describe a privacy risk response that is proportionate to the level of risk posed.**

This may include reference to the measures to protect the Sensitive Personal Information (contractual, physical, technical, administrative measures) you outline elsewhere in this PIA. Privacy risks below are examples only; add new rows if necessary.

| Privacy risk                                       | Impact to individuals or Camosun College | Likelihood/risk response/mitigation |
|----------------------------------------------------|------------------------------------------|-------------------------------------|
| Unauthorized collection of PI by Camosun employees | Low/medium                               | Unlikely                            |
| Unauthorized use of PI by Camosun employees        | Low/medium                               | Unlikely                            |
| Unauthorized disclosure of PI by Camosun employees | Medium/high                              | Unlikely                            |
| Unauthorized collection of PI by Third Party/ies   | Medium/high                              | Unlikely                            |

|                                                  |      |          |
|--------------------------------------------------|------|----------|
| Unauthorized use of PI by Third Party/ies        | High | Unlikely |
| Unauthorized disclosure of PI by Third Party/ies | High | Unlikely |

**\*Note: the Privacy Office has a Privacy Breach system in place .**

## PART 6: PROTECTION

Please share how the initiative will secure Personal Information to protect personal 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.

**30.** Does your initiative involve digital tools, databases, or information systems?

☒ Yes ☐ No

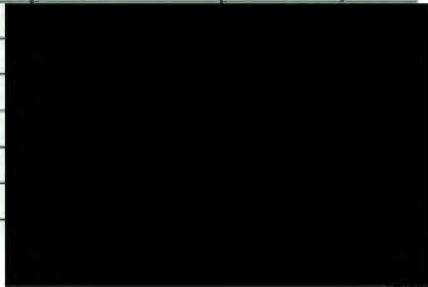
**31.** What **physical security** safeguards are in place to protect Personal Information in this initiative?

Identify the elements of physical security that protect where the records for your initiative are stored (Check all that apply. Specify, "Other" if applicable)

| Safeguard                                                  | At Camosun                          | At Third Party           |
|------------------------------------------------------------|-------------------------------------|--------------------------|
| Restricted access to property (i.e. key card access)       | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Security monitored building                                | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Key locks and door astragals                               | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Locked filing cabinets                                     | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| "Clean desk" practices                                     | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Security officers                                          | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Security cameras                                           | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Other: <b>See Vendor HECVAT report for further details</b> | <input type="checkbox"/>            | <input type="checkbox"/> |

**32.** What **technical security** safeguards are in place to protect Personal Information in this initiative?

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)

| Safeguard                                                   | At Camosun                                                                            | At Third Party |
|-------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------|
| Authentication control: Strong Password Management          |  |                |
| Authentication control: Multi Factor Authentication ("MFA") |                                                                                       |                |
| Role-based access                                           |                                                                                       |                |
| Encrypted in transit                                        |                                                                                       |                |
| Encrypted at rest                                           |                                                                                       |                |
| Isolation Control: Application                              |                                                                                       |                |
| Isolation Control: Network                                  |                                                                                       |                |

|                                                     |
|-----------------------------------------------------|
| Isolation Control: Database                         |
| Vulnerability Scanning                              |
| Vulnerability Penetration Testing                   |
| <b>See Vendor HECVAT report for further details</b> |



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

Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

| Safeguard                                                                                                            | At Camosun                          | At Third Party                      |
|----------------------------------------------------------------------------------------------------------------------|-------------------------------------|-------------------------------------|
| Agreement/Contract                                                                                                   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Privacy/Data Protection Policy                                                                                       | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Documented business practices and processes for proper collection and management of Personal Information             | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Privacy training specific to the initiative                                                                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Cybersecurity Training                                                                                               | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| Staff Security Awareness Training                                                                                    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Dedicated Information Security Staffing                                                                              | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Information Security Policy                                                                                          | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Vendor Third Party Compliance and Certifications (i.e. ISO, SOC Type 2, CSA, PCI DSS, SOX) – <b>yes – SOC Type 2</b> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| Security Incident Response Plan                                                                                      | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Camosun College – Standards of Conduct Policy O-5.11 [employees]                                                     | <input checked="" type="checkbox"/> |                                     |
| Camosun College – Protection of Privacy Policy O-6.1                                                                 | <input checked="" type="checkbox"/> |                                     |
| Camosun College – Systems and Networks Administration O-1.2                                                          | <input checked="" type="checkbox"/> |                                     |
| Camosun College – Acceptable Technology Use Policy O-1.1 [network use]                                               | <input checked="" type="checkbox"/> |                                     |
| Other: <b>See Vendor HECVAT report and supporting eRez policies for further details</b>                              | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

**34. If the initiative involves a Third Party, please indicate what type of Agreement governs the relationship between Camosun College and the Third Party. Please select one.**

- ☐ Camosun College GSA (negotiated Agreement between Camosun College and the Third Party)
- ☒ Vendor's Agreement (negotiated Agreement between Camosun and the Third Party)
- ☐ Online "Terms of Service" or "Terms of Use" (often non-negotiable)
- ☐ Memorandum of Understanding/Memorandum of Agreement ("MOU"/"MOA")
- ☐ Other (specify):
- ☐ No Agreement

**35. If the initiative involves a Third Party, does an End User License Agreement ("EULA") apply to the individuals whose Personal Information is involved?**

- ☒ Unknown

36. The Privacy Officer will need to review all draft/proposed Contracts/Agreements (and related materials, i.e. contract appendices/schedules; Third Party privacy policies or online terms and conditions, if any) involved in the initiative. Have you ensured these have been provided? Check only one.
- ☒ Yes                                      ☐ No                                      ☐ N/A (No Third Party involved)
37. Where are the privacy related terms referenced in the contract or agreement if applicable? (Check all that apply)
- ☒ In the body of the contract or agreement  
☒ Third Party will sign Camosun College's Privacy Protection Schedule for Cloud Services  
☐ Third Party will sign Camosun College's Data Security Schedule  
☒ In the Third Party's privacy or data protection policy or appended schedules  
☐ In a separate Information Sharing Agreement  
☐ There are no privacy related terms in the contract or agreement (or related documentation)  
☐ There is no contract or agreement for this initiative yet.
38. Controlling and tracking access
- Review each strategy below that describes how to limit or restrict who can access Personal Information and how to keep track of who has accessed Personal Information in the past. Check all that apply. Specify "Other" if applicable.
- ☒ Managed role-based access to Personal Information for Camosun College employees  
☐ Managed role-based access to Personal Information for Third Party  
☐ Third Party access is time limited for installing, implementing, maintaining, repairing, troubleshooting, or upgrading an electronic system  
☐ Third Party access escorted by authorized Camosun College employee  
☐ Audit logs at Camosun College  
☐ Audit logs from Third Party  
☐ Other: *(fill in details)*
39. Artificial Intelligence ("AI"): Are you aware whether this initiative actively incorporates or uses any AI features? If yes, please contact the Camosun College Privacy Office at [privacy@camosun.ca](mailto:privacy@camosun.ca).
- ☐ Yes                                      ☒ No                                      ☐ Unknown

## 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.

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.

40. How will Camosun College 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 Camosun College
  - ☐ Software or service uses automated processes to enter and manage Personal Information
  - ☒ Unknown – the entire process is not yet known.
  - ☐ Other: *(fill in details)*
41. Is there a documented process in place to correct Personal Information?
- ☒ Yes ☐ No
42. 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)
43. If there is a request for correction from an individual and Camosun College or the Third Party disclosed that individual's Personal Information in the last year, FIPPA requires that Camosun College or the Third Party provide the applicable other public body or Third Party about the request for correction. Will Camosun College or the Third Party ensure that these notifications are done when necessary?
- ☒ Camosun College will forward correction notifications
  - ☐ Third Party will forward correction notifications
  - ☐ Camosun College 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.

- 44.** How long will Camosun College 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.

Colleague information kept indefinitely.

- 45.** How long will the vendor 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.

Vendor will keep indefinitely unless contract expires.

- 46.** 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)

- ☒ Schedule records review and disposition dates in Outlook calendars
- ☒ Build conditions for disposal into department Standard Operating Procedures
- ☒ Send direct written communication to staff or service providers.

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

- ☐ Camosun College business unit shredding on campus
- ☐ Camosun College contracted shredding service provider
- ☒ Camosun College deletion of electronic record(s)
- ☒ Service Provider shredding/deletion of record(s) under Camosun College contract
- ☒ Service Provider shredding/deletion of record(s) under Camosun College written Instruction
- ☐ Other (explain):
- ☐ Other (explain):

## PART 9: INFORMATION FLOW

### 48. 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.

The Privacy Officer will complete column 3 to identify the legal authority you have for the collection, use or disclosure.

| Information Management Steps                                                                                     | Collection, use or disclosure | FIPPA |
|------------------------------------------------------------------------------------------------------------------|-------------------------------|-------|
| Step 1: Collected directly from the student.                                                                     | collection                    | 26(c) |
| Step 2: Information used to manage housing operations.                                                           | use                           | 32    |
| Step 3: Not to disclose the Personal Information inside or outside Camosun College unless authorized under FIPPA | disclosure                    | 33    |
| Step 4:                                                                                                          |                               |       |

## PART 10: TRAINING

### 49. 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 Camosun College unless authorized under FIPPA
- ☐ Storage: To store the Personal Information only in Camosun College-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 (if used on or on behalf of Camosun to make a decision that directly affects the individual) – with longer retention periods only when necessary
- ☒ Disposal: To dispose, when applicable, in a secure method that renders the Personal Information permanently irretrievable

## PART 11: PERSONAL INFORMATION BANKS

50. 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

## PART 12: OIPC REVIEW REQUIREMENTS (Privacy Officer to Complete)

51. Is this initiative a data-linking program under FIPPA? If this PIA addresses a data-linking program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.
- ☐ Yes ☒ No
52. Is this initiative a common or integrated program or activity? If this PIA addresses a common or integrated program, this PIA must be submitted to the Office of the Information and Privacy Commissioner.
- ☐ Yes ☒ No

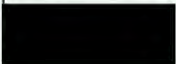
## PART 13: PRIVACY OFFICE(R) COMMENTS

This PIA is based on a review of the material provided to the Privacy Office(r) as of **[enter date]**. 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).

[Additional Space for customized Privacy Officer Comments]

### Privacy Office Signature

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

| Name and Title                | Signature                                                                           | Date signed       |
|-------------------------------|-------------------------------------------------------------------------------------|-------------------|
| Ann Behennah, Privacy Officer |  | December 10, 2025 |

## PART 14: APPROVAL SIGNATURES

### Institution Signatures

This PIA is compliant with FIPPA when it accurately 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 Privacy Office, 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 Privacy Office 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 employees are trained on and able to comply with their obligations under FIPPA; related College policies and procedures; and Camosun College Privacy Office recommendations relative to this initiative.

#### Signature of Initiative Lead

| Name and Title                                    | Signature                                                                                             | Date signed |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------|
| Evan Hilchey, Interim Associate VP Administration | Evan Hilchey<br><small>Digitally signed by Evan Hilchey<br/>Date: 2026.02.12 15:23:32 -08'00'</small> | 2/12/26     |

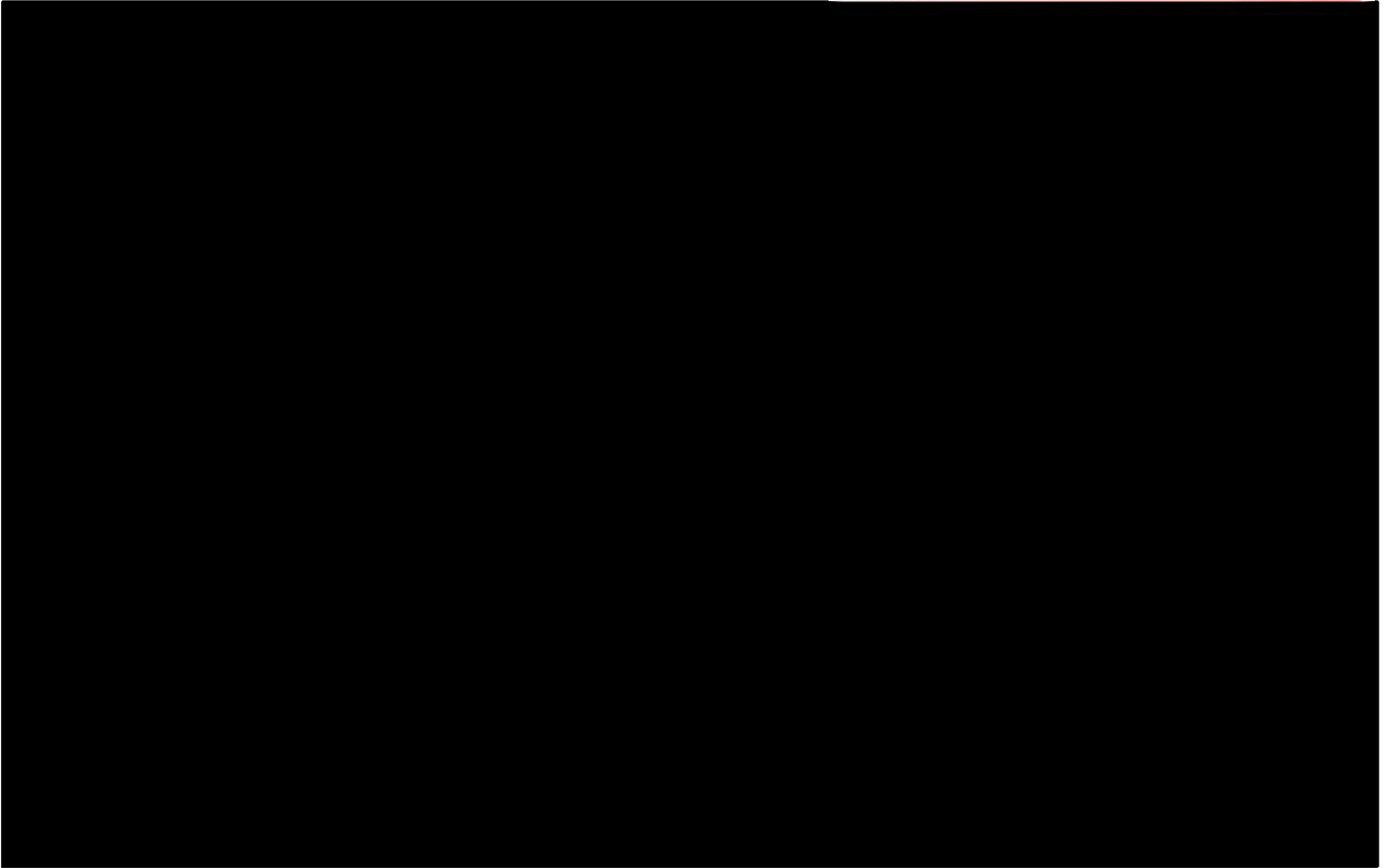
**Declaration of Information Security:** (Required only when college initiative involves Information Security considerations).

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 Camosun College business information described in this PIA.

#### Signature of Information Security

| Name and Title                                        | Signature                                                                                                               | Date signed |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------|
| Farzaan Nusserwanji, Associate Director, ITS Security | Farzaan D Nusserwanji<br><small>Digitally signed by Farzaan D Nusserwanji<br/>Date: 2026.02.13 11:29:00 -08'00'</small> | 2/13/26     |

## Appendix A



s. 15(1)(l), 21