Privacy Impact Assessment
Term Hire Workflow Project (2023)

Part 1 – General

Name of Department/Branch:	Vancouver Community College Continuing Studies			
PIA Drafter:	Norman Chang, Michael Peterson			
Email:	nchang@vcc.ca	Phone:	604-868-1068	
Program Manager:	Michael Peterson			
Email:	mipeterson@vcc.ca	Phone:	778 836-3275	

In the following questions, delete the descriptive text and replace it with your own.

1. **Description of the Initiative**

   In January 2023, scores of employment contracts were delayed as a result of weak monitoring systems and manual workflows that were dropped due to human error. For Fall 2023, People Services has developed a contract-processing system that leverages our existing IT systems to modernize our process and improve how these contracts are handled.

   There are three main objectives for the new system:

   - Improved reliability of workflows (make sure new contracts are not missed or delayed at any stage of the processing workflow).
   - Improved transparency of workflows (make it easier for authorized parties to know the status of a contract as it progresses through each stage of the processing workflow).
   - Faster overall processing of each contract.

   After months of research, experimentation, and discussions with peer institutions, we have decided to modernize the existing contract workflow using VCC's existing licenses for Microsoft SharePoint and Microsoft Power Automate.

   This solution is expected to be in place from August 2023 – October 2025.

2. **Scope of this PIA**

   This PIA covers the pilot and subsequent rollout phases. The responses within this PIA should assist in analyzing the possible impacts on employee privacy, describing privacy design techniques and risk mitigation measures in place as a part of the solution and ensuring that privacy

considerations are first and foremost in the design of the proposed system and within the project overall. Followings are the technology scope covers by the project:

Data Location	Access	Infrastructure
On Dept Head CPU	VCC Authentication	Unknown, VCC Authentication
On SharePoint 1	VCC Authentication – Wide	VCC - Microsoft Environment
On SharePoint 2	VCC Authentication – Narrow	VCC - Microsoft Environment
On SharePoint List	VCC Authentication – Narrow	VCC - Microsoft Environment
On Automate Flows	VCC Authentication – Admins	VCC - Microsoft Environment
On Approval Request	Select pre-populated Email	VCC - Microsoft Environment
On Approval Response	Dynamic Email	VCC - Microsoft Environment
On Notification Emails	Dynamic Email	VCC - Microsoft Environment

3. Related Privacy Impact Assessments

We are unaware of any PIA concerns associated with MS SharePoint or Automate. The use of MS product suite is covered by the BCNET PIA.

BC PIA for MS
Cloud Services.pdf

4. Elements of Information or Data

(Elements of information or data utilized based on implementation of service.)

Account Information about User	Per VCC user account
Identifying Information about candidate (existing employees)	Employee Name Employee Number Particulars of Employee Credentials (Meets Criteria, Recommended by Committee, Previous Experience teaching in Area)
Particulars of Employment Contract	Particulars of Employment Contract (start/end/assignment/total hours/specific days worked)
Particulars of Employee	Particulars of Employee Compensation (Step

Compensation	Placement/benefits eligibility)
Contract Approve/Reject	Dean's response to approval request, with rationale.
Processing Response Times	System allows for timestamps for task arrival/completion at each stage of processing.

Part 2 – Protection of Personal Information

5. **Storage or Access outside Canada**

Microsoft Sharepoint is hosted 100% in Canada. Microsoft Automate, a workflow engine, has only a US data center. The complete solution will have data travel between US and Canada country boundary.

With the potential data travel to or store within US for this service, employees will need to perform explicit acknowledgement and acceptance of the storage country:

For a given PSI, its data is only accessible by:

    1) Authorized Staff of that PSI (i.e. graduations / student admin / admissions)

    2) Employees, who can access only Official Documents issued to them

    3) Third Parties, with whom Official Documents have been shared, at the explicit request of the Employee associated with the document.

Privacy Impact Assessment
Term Hire Workflow Project (2023)

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	Yes
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	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.	no
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

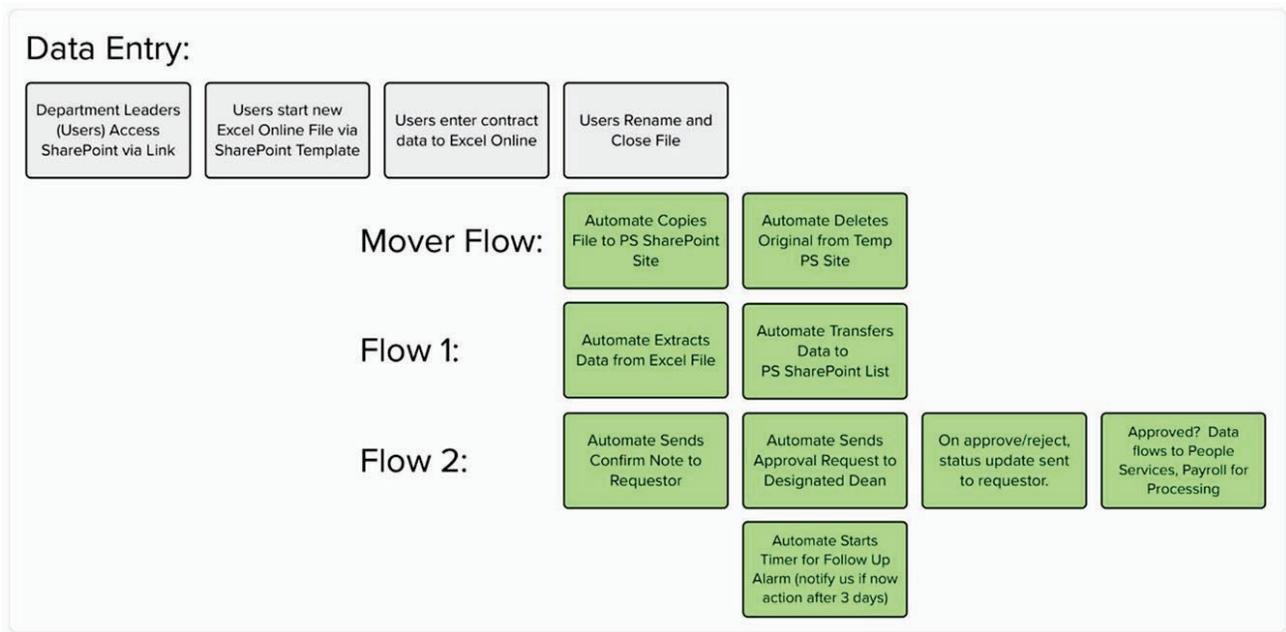6. **Common or Integrated Program or Activity***

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
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; **Notes: EPBC integration is not in scope.**	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. **Personal Information Flow Diagram and/or Personal Information Flow Table**

8. **Risk Mitigation Table**

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	*Employees could access personal information and use or disclose it for personal purposes*	*Staff and contract instructors bound by employee/contractor agreement; staff bound by Standards of Conduct*	*Low*	*High*
2.	*Hosted infrastructure compromised*	*Comprehensive infrastructure design, monitoring and alerts. Data and documents encrypted in transit and at rest with secure key storage.*	*Low*	*High*
3.	*Client's personal information is*	*Transmission is encrypted.*	*Low*	*High*

	compromised when transferred to the service provider			
4.	*Injection attack*	*Secure development and deployment policies and practices. Monitoring, Scanning and alerts.*	*Medium*	*High*
5.	*Exploiting vulnerabilities in libraries, frameworks, and other dependent software components*	*Monitoring and subscribing to known threat lists and pursuing an aggressive patch management policy. Regular vulnerability scanning.*	*Medium*	*High*
6	*Brute-force authentication attack*	*Limiting authentication attempts and introducing reCaptcha for multiple attempts. MFA for highly sensitive operations such as document issuing.*	*Medium*	*High*

9. **Collection Notice**

If your initiative is collecting personal information directly from 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.*

VCC privacy notice:

VCC privacy page link is added to the footer on every page of the website:

https://www.vcc.ca/about/college-information/privacy-policy/

Within the above policy, a summary of the approach has been provided with link to disclaimer as well as contact information (#3).

In addition, all service users for this project will need to perform additional explicit acknowledgement, consent and acceptance to data usage and storage location .

Under What Authorization We Collect (#2)

We collect personal information from you as authorized by the College and Institute Act. The personal information we collect is necessary to:

- *obtain a personal education number (PEN) for the student*

- *carry out institutional responsibilities related to operating program or activity*

- *prepare and submit budgets, financial statements, reports and other information that the minister considers necessary to carry out the minister's responsibilities in relation to institutions*

- *conduct institutional research and statistical analysis*

The Freedom of Information and Protection of Privacy Act has directed that we provide you with this background. You may be assured that we will take all reasonable measures to ensure that your information is treated in a confidential manner.

Why We Collect (#1)

There are three main objectives for the new system:

- *Improved reliability of workflows (make sure new contracts are not missed or delayed at any stage of the processing workflow).*

- *Improved transparency of workflows (make it easier for authorized parties to know the status of a contract as it progresses through each stage of the processing workflow).*

- *Faster overall processing of each contract.*

Part 3 – Security of Personal Information

If this PIA involves an information system, or if it is otherwise deemed necessary to do so, please consult with the Privacy Officer, CIO or IT Security Officer when filling out this section..

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

The solution is hosted entirely on cloud infrastructure provided by Microsoft. Microsoft employs a number of complex physical security mechanisms around a layered security approach.

https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

EMPLOYEE DATA CENTER ACCESS

Access to physical datacenter facilities is tightly controlled by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, integrated alarm systems, around-the-clock video surveillance by the operations center, and multi-factor access control. Only required personnel are authorized to access Microsoft datacenters. Logical access to Microsoft 365 infrastructure, including customer data, is prohibited from within Microsoft datacenters.

MS Security Operations Centers use video surveillance along with integrated electronic access control systems to monitor datacenter sites and facilities. Cameras are strategically positioned for effective coverage of the facility perimeter, entrances, shipping bays, server cages, interior aisles, and other sensitive security points of interest. As part of our multi-layered security posture, any unauthorized entry attempts detected by the integrated security systems generate alerts to security personnel for immediate response and remediation.

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

The entire solution runs within a tightly controlled, managed, and partitioned Microsoft environment. All aspects of Microsoft physical and infrastructure-level security are outlined on:

https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

12. Does your branch/department rely on any security policies?

VCC IT Security Policies:

Information Technology General Policy (B.5.1, B.5.2, B.5.4, B.5.5)
https://www.vcc.ca/about/governance--policies/policies/administration-policies/

Other IT Policies:

IT Administrative Rights Application and Policy
https://employee.vcc.ca/media/myvcc/content-assets/documents/departments/information-technology/forms/it-Administrative-Rights-Policy.pdf

Vulnerability Management
https://employee.vcc.ca/media/myvcc/content-assets/documents/departments/information-technology/other/Vulnerability-Management-IT-Standard.pdf

13. **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.**

Multiple security controls ensure that only VCC staff is able to access and control its own portal and to access Official Documents within its repositories. VCC Portal login requires 2-factor authentication using Azure active directory. The 2-factor authentication mechanism is mandatory for all resource access. Role based access controls further dictate what users can perform what actions within the system.

All actions are recorded in an audit trail within Sharepoint.

14. **Please describe how you track who has access to the personal information.**

Within the Term Hire Workflow project, all activities and accounts are fully audited (login, logout, access document, share document, verify document, change password, link account, etc.). Each event records the affected user, activity, and a time stamp. These can then be viewed by the Sharepoint administrator.

Within the project, the application records all login/logout, document issuing, viewing, revocation, deletion, as well as admin operations such as user creation, update, permission/role assignment or change. Affected user, IP address, and times tamp are recorded for each event.

Part 4 – Accuracy/Correction/Retention of Personal Information

15. **How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?**

Users information will not be disclosed to public but individuals defined within the business processes. VCC HR will handle all questions and requests in regard to data update or discrepancies.

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

No.

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

N/A

18. 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

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

VCC does not share data within this application with other entities.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	

20. Does the program involve access to personally identifiable 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 your privacy office(r).	

21. 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

A personal information bank of employee information will be created. VCC is able to provide the descriptors required as part of this initiative.

As per section 69 (6) of FOIPPA:

> *(6) The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:*
> > *(a) its title and location;*
> > *(b) a description of the kind of personal information and the categories of individuals whose personal information is included;*
> > *(c) the authority for collecting the personal information;*
> > *(d) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;*
> > *(e) the categories of persons who use the personal information or to whom it is disclosed;*

Refer to question 4 for data descriptors.

Part 6 – Privacy Office(r) Comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update

Part 7 – Program Area Signatures

Director Special Projects	Signature	Date

Privacy Officer	Signature	Date

Director IT	Signature	Date