Privacy Impact Assessment

MyCreds Credential Wallet

Part 1 – General

Name of Department/Branch:	Vancouver Community College Continuing Studies		
PIA Drafter:	Norman Chang		
Email:	nchang@vcc.ca	Phone:	604-868-1068
Program Manager:	Adrian Lipsett		
Email:	alipsett@vcc.ca	Phone:	604-443-8392

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

1. Description of the Initiative

myCreds is a Canadian platform that is supported by ARUCC (Association of Registrars of Universities and Colleges of Canada) and works with Digitary, suggesting that myCreds is likely to become the de-facto digital credential environment nationally. Dozens of Canadian institutions have already gone live with myCreds (e.g., Lambton College), and many others are in the process of examining the platform or have signed contracts (e.g., KPU, Douglas, UNBC). In addition, both AEST and EPBC are actively working with the myCreds team.

Badging remains a strategic and beneficial initiative for the College as it provides a tangible bridge to effectively convey our students' competencies to prospective employers and educational opportunities beyond VCC. As myCreds links with Banner (a D1 integration is being developed as well) to confirm individual students' educational achievements, students across VCC would be able to access and share their badges wherever and whenever they wish– thus extending the value that our credentials provide.

The Association of Registrars of the Universities and Colleges of Canada (ARUCC) owns the ARUCC National Network and is subject to the Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) as a federally incorporated not-for-profit. However, the vendor that provisions the Solution and Services for ARUCC to support the ARUCC National Network will be required to connect and move information between the ARUCC National Network and Canadian provincial application centres, transcript hubs, and post-secondary institutions that a re subject to provincial privacy regulations.

Digitary's CORE platform, which is the basis for myCreds, enables:

a. PSI to issue Official Documents (Transcripts, Parchments, Official Letters, etc.) as well as microcredentials (open badges) to Learners in a secure, controlled manner.

b. Learners to login, access, and share their Official Documents and badges in a variety of simple and secure ways.

c. Third Parties to verify shared Official Documents and badges in a variety of secure ways that require explicit Learner consent for the disclosure of a Learner's Personally Identifiable Information (PII)

Digitary CORE employs a unique hub and spoke design that is both a Learner-centric Official Document model and a national-scale data exchange Network. This pattern has been proven at scale across a wide variety of international PSIs in Ireland, UK, Australia, and New Zealand - countries with strict regulatory data privacy and security. By employing a hub and spoke pattern, combined with an cryptographic issuance model for credentials, the Digitary CORE architecture meets current needs (data exchange) whilst laying the foundation for a smooth transition to emerging technologies as they mature including Self-Sovereignty and W3C Verifiable Credentials. Digitary CORE is based on the concept of privacy by design, minimizing privacy risks by building in privacy into the architecture of its system.

From a technical perspective, the myCreds will essentially be an instance of the Digitary CORE platform, hosted 100% in AWS Canada, with a Canadian skin applied to it.

2. Scope of this PIA

This PIA covers the pilot and subsequent rollout phases of myCreds using the Digitary CORE platform. The responses within this PIA should assist in analyzing the possible impacts on learner 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.

AWS is outside the scope of this PIA.

Elluician Banner is outside the scope of this PIA.

Active Directory (AD) is outside the scope of this PIA.

3. Related Privacy Impact Assessments

Previous PIAs were completed for a similar solution and service across Ireland as well as for the My eQuals project (https://www.myequals.edu.au/) for Australia and New Zealand.

The use of AWS is covered by the BCNET PIA.

2017 BCNET AWS PIA.doc

4. Elements of Information or Data

Data may include name, address, phone number, school email address, personal email address, single sign on identifier, registration information, IP address, web browser, student number, student records, etc.

Each Official Document issued through myCreds by VCC requires a minimum set of metadata fields in order to identify the Learner associated with the document, so that the learner can access it via the Portal:

- Full name
- Email address
- Student Identifier

VCC may include additional, optional metadata fields to enable easier searching and reconciliation of Official Documents within the platform.

The content of each Official Document is a matter for the issuing PSI and there are no minimum requirements per se. Official Documents are represented in most cases as PDFs and so the relevant data is encoded as such inside the PDF. Where the Official Document is generated from structured da ta (i.e. XML, CSV), those data fields are embedded as attachments within the Official Document.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

The entire solution is hosted 100% in Canada along with all associated data. For a given PSI, its data is only accessible by:

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

2) Learners, 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 Learner associated with the document.

In cases where a learner initiates a document share to an entity outside of Canada, the document becomes available outside of Canada. The type of share the learner creates will determine how the document is consumed. For instance, a platform *Network Share* makes the document available to a recipient through their own attached Digitary portal; a URL share links the recipient back to the portal hosted in Canada where they can access the document from where it resides.

In addition, Digitary's support team can access the data in order to maintain support coverage as per SLAs. In this context, Digitary support coverage from outside Canada is usually limited to core infrastructure and associated components only. There may be instances where access to further information is required to remediate a problem. In such cases where an issue may require access to PII and where specific permission does not exist for the team outside of Canada to access that information for that issue, the support request will be exclusively managed from the Canada office. The aim remains to address and resolve the issue within existing SLAs. It should also be noted that needing access to PII is usually an exception in any case and that all PII is encrypted and not readily accessible to any member of the team.

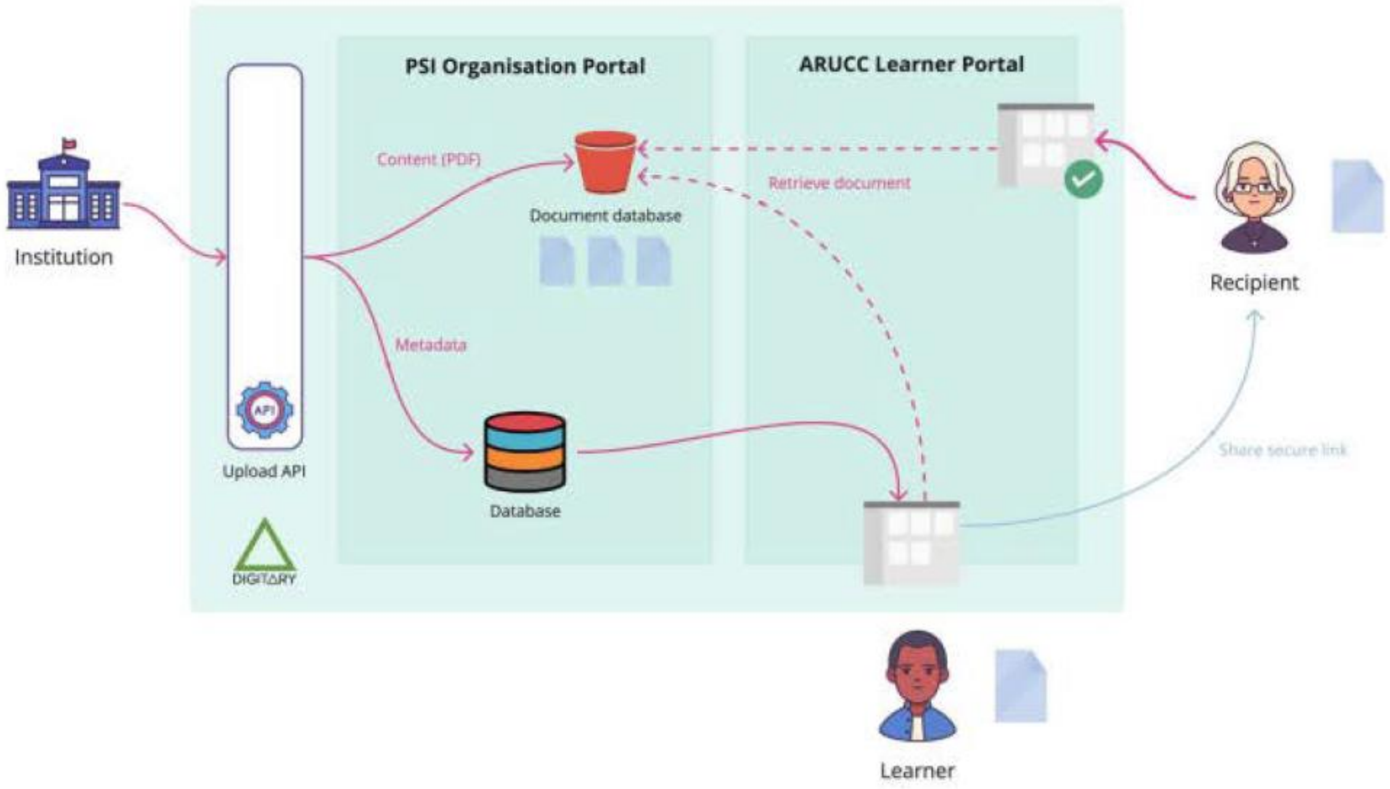
6. Data-linking Initiative*

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.	

7. 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.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table



1. Documents are uploaded by VCC using either an API or manual upload through the user interface.

2. Documents are signed and issued to learners

3. Learners pick-up documents and share them with third party recipients through the platform (either via URL or sent via the Network)

4. Recipients can verify back-to-source through the platform share URL (or receive via the Network to an inbox or API endpoint)

9. 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 compromised when transferred to the service provider*	*Transmission is encrypted over TLS (vl.2) and access is locked down to whitelisted source IPs, with user/service authentication as appropriate*	*Low*	*High*
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*

10. 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.*

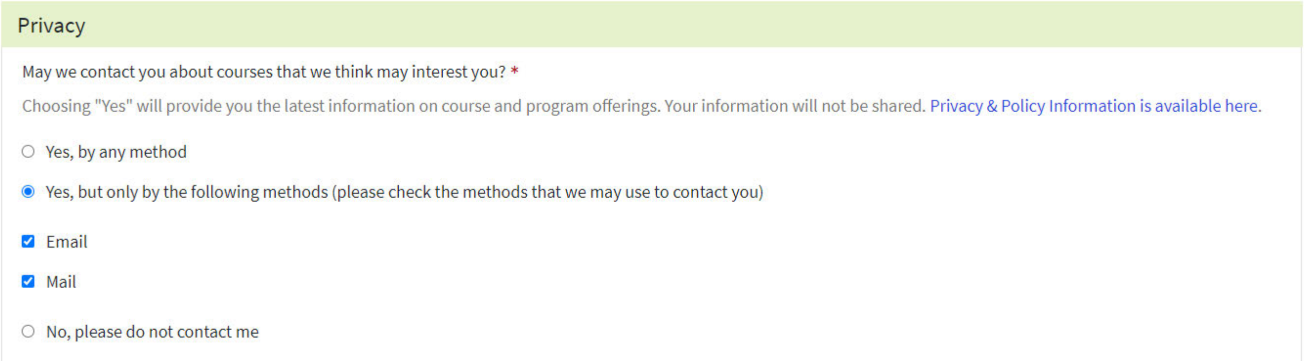
VCC privacy notice:

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, new students will necessarily be required to review and confirm their preferences with regard to subsequent marketing communications from VCC, and are provided with a link to our privacy policy as part of their initial account creation (see screenshot below). They are able to review this policy and make changes to their communication preferences at any time within the Student Portal > My Profile > Privacy.



Privacy

May we contact you about courses that we think may interest you? *

Choosing "Yes" will provide you the latest information on course and program offerings. Your information will not be shared. Privacy & Policy Information is available here.

○ Yes, by any method

● Yes, but only by the following methods (please check the methods that we may use to contact you)

☑ Email

☑ Mail

○ No, please do not contact me

More detail information is included under the information disclaimer section:

https://www.vcc.ca/about/college-information/disclaimer/

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)

We collect personal information:

- *For the purpose of sending you official correspondence related to your education at VCC, communicating with you in an instructional capacity, and gathering essential information for operating purposes.*
- *For the purpose of providing students with the opportunity to participate in former student outcome surveys. The results of these surveys are used to improve the quality and effectiveness of instruction and services that we provide.*

The Ministry uses this information in order to monitor institutional progress and comply with government stated objectives.

To conduct institutional research on education policy issues, such as quality of education, student satisfaction, ease of transfers, student access, future student needs, evaluate training needs for a variety of population groups such as insert students, transfer students, first nations students, international student etc.

Digitary privacy notice:

myCreds clearly indicates the location of the Digitary Privacy Policy that outlines the terms of the service, the data collected and its use. Please refer to the following URL for the current Digitary Privacy Policy:

https://core.digitary.net/#/privacy

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..

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

The solution is hosted entirely on cloud infrastructure provided by Amazon Web Services (AWS). AWS employs a number of complex physical security mechanisms around a layered security approach. Further information on AWS data centers and their layered security model can be found at the URL below.

https://aws.amazon.com/compliance/data-center/data-centers/

EMPLOYEE DATA CENTER ACCESS

AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

THIRD-PARTY DATA CENTER ACCESS

Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

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

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

http://aws.amazon.com/security

The AWS compliance program ensures that all AWS services remain aligned with and compliant against number of local (for resident operations and data centres) and international standards and certifications. AWS standards and certifications include Canada' s Federal Private Sector Privacy Legislation (PIPEDA). Further information is available at the URLs listed below:

https://aws.amazon.com/compliance/programs/

https://aws.amazon.com/compliance/pipeda/

In December 2019, the Canadian Government signed a framework agreement with AWS to provide secure cloud services. Further information on the Canadian Government assessment performed and service applicability is available at the following locations:

https://aws.amazon.com/canada/publicsector/cloud-contract/

https://aws.amazon.com/blogs/publicsector/aws-now-able-to-host-protected-b-data-for-the-government-of-canada/

A key takeaway from the above published documents is out lined below.

"In order to meet the high security standard required by the Government of Canada, the AWS Canada (Central) Region was assessed against hundreds of controls. This security assessment provides additional assurance to customers of all sizes and across all industries, including local and provincial governments, that AWS has passed a significant technical review set forth by the Government of Canada."

Within the AWS shared responsibility model, Digitary manages its part of the overall solution as follows.

Firstly, all environments (FIT, UAT, PROD) run on separate AWS accounts. For each environment:

s. 15(1)(l)

[redacted]

s. 15(1)(l)

[redacted]

13. 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

myCreds Security framework:

Digitary's Information Security Framework follows their alignment and formal work towards ISO27001 accreditation, alignment to SOC2 and their commitment to GDPR and includes the following:

- *Roles and responsibilities*
  - *Clear identification of all relevant roles*
  - *Descriptions of specific responsibilities as they relate to each role regarding information management and security*
- *Hiring policies and frameworks*

  o Procedures to be completed prior to hiring - i.e. relevant reference and police checks

  o Contractual terms and conditions as they relate to information security

  o Procedures for onboarding and departure

- *o Procedures for disciplinary action where information security guidelines have been compromised*

- *Information Classification*
  - *o Public, Internal, Restricted, Confidential levels of classification*
  - *o Impact assessment of breach at any level*
  - *o Access rules for each listed level*
  - *o Storage of information for respective classifications*
  - *o Transmission rules governing dissemination of data at the different classification levels*
  - *o Disposal of data at the different classification levels*
- *Media handling*
  - *o Describes the policies and controls governing the handling of removable media*
  - *o Controls governing the safe and secure physical media transfer*
  - *o Controls and adherence to physical media disposal policies*
- *Cryptographic control policies*
  - *o Encryption, storage, and access controls for secure key management*
  - *o Policies on secure device modules*
- *Access controls*
  - *o System administrator policies*
  - *o User policies - rights management and removal*
  - *o External information systems and networks usage*
- *Security Training*

o Training and testing of new employees prior to handling sensitive information or accessing systems

o Periodic training and testing to ensure continuous awareness and compliance

- *Systems Administration*

o General patch management guidelines for operating systems and related components with ongoing alerts addressed as required depending on patch severity

o Detected or reported application vulnerabilities are patched immediately or as indicated depending on their severity

o Controlled and audited access to systems, data, configurations, logs, and access credentials

- *Secure Development Policies*

o All Infrastructure, application, configuration, and credentials are securely managed through version control system with comprehensive auditing

o Clear articulation of roles and responsibility regarding secure software development

o Training and guidelines on common vulnerabilities, procedures and secure development methodologies including OWASP

o OWASP principles enshrined in development and testing frameworks with high-level policy checklists built into the testing and release process of all Digitary systems

o Pre-release internal penetration testing of all releases using the Burp Suite cybersecurity toolkit - this is a licensed purchased version, not the free version.

o External audits and penetration tests are performed at least annually

o Early identification of security concerns in feature development and ensuring the relevant test scenarios exist to validate them as part of our agile development process.

o Secure code guidelines are reviewed often in line with technical developments and the evolution of Digitary's platform and supporting technology.

  - *Peer-review of all application code prior to merging with development branches.*
  - *Ongoing and frequent formal team code review session*

- *Incident response*
  - *Clear roles and responsibilities as they relate to information security incidents*
  - *Reporting and distribution of information for security events*
  - *Procedures and responses to information security events*
  - *Incident response planning guidelines*
  - *Automated 24/7 monitoring and alert mechanisms exist to ensure that relevant members are immediately aware of security issues as they happen, include:*
    - *Site 24/7 monitoring - application uptime and SLA monitoring*
    - *Sumologic - application log consolidation and security alerts*
    - *AWS CloudWatch - infrastructure alerts*
    - *Alertlogic- security monitoring and alerts including SOC*
- *Backup, disaster recovery (DR) and business continuity (BC)*
  - *Policies and procedures outlining the backup frequency, location, restore plans*
  - *DR planning including locations, testing frequency and procedures*
  - *Monitoring and alert mechanisms to ensure minimal disruption in line with SLAs*
- *Privacy policies*
  - *Digitary compliance against GDPR*
  - *Policies covering how Digitary collects information, how it used, how it is secured, how (if at all) specific information is shared as well as relevant user controls to support this*

- *Audits and Testing*
  - *DR tests are conducted annually*
  - *Security tests are conducted with every release*
- *Third-party partners and contractors*
  - *All partners and contractors are assessed using the same security and privacy tests performed across the business*

Here is the introduction to ISO 27001:

Infosec_101v1.1.pdf

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.

Multiple security controls ensure that only VCC is able to access and control its own portal and to access Official Documents within its repositories. s. 15(1)(l) Role based access controls further dictate what users can perform what actions within the system.

s. 15(1)(l)

All actions are recorded in an audit trail within the Digitary applications. s. 15(1)(l)

Learners must login to a secure web portal to access their Official Documents once they have been issued by VCC via the corresponding VCC Portal. Documents are not accessible to third parties at this stage. Learners then have control over who they share their Official Documents with, and for how long. Transmission over the network by default is initiated by the Learner. Third parties can only access Official Document(s) that have been shared with them by a Learner.

From a support perspective, specific access to production systems is restricted to selected Digitary team members on a least-privilege basis. Requests for access must be made through the relevant team leads in response to a valid ticket from our Zendesk platform, or independently following senior management approval.

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

Application-space auditing:

Within the VCC MyCreds space, all activities on Learner's Official Documents and accounts are fully audited (login, logout, access document, share document, verify document, change password, link account, etc.). Each event records the affected user, document, source IP of the initiator, and a time stamp. These can then be viewed by the Learner within their account.

Within each PSI Portal, 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. By design, Learner sharing activity is not passed to the PSI to preserve the Learner's privacy.

System-space auditing:

Access events to applications (standard HTTP logs) are taken for all application endpoints. Digitary's internal applications also log certain information to assist with error analysis. s. 15(1)(l) [redacted]

Access to underlying AWS systems and services within Digitary's control is recorded by Digitary for management and security purposes. s. 15(1)(l) [redacted]

s. 15(1)(l) [redacted]

All system logs have a one year retention period.

Bottomline solution provides complete tracking across the platform. Access to the system is fully auditable and provides complete details on user system access across VCC portal as well as Learners interfacing through the public Digitary Learner Portal. All document interactions are recorded. This includes the issuing, signing, viewing, and sharing of any loaded artefact into the system. PSI Portal access is especially sensitive with all major operations maintained as auditable logs including administration functions that alter the overall state of the system.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. **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 have the ability to update their personal information via VCC myCreds portal.

    Issued Official Documents can be updated by VCC only. Where a new Official document is generated and re-issued as a replacement to an existing one, the learner is notified that the document has been updated and replaced via automatic email. Official Documents issued through the platform cannot be altered within the platform.

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

    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 and complete.**

    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.

The platform supports the sharing of learner Official Document with other entities including government, hubs, and schools in order to support their onward learning or employment journey. These interactions are learner initiated and the learner remains at the center of all actions where their documents are shared.

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).	

21. 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).	

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

A personal information bank of student information will be created in MyCreds. 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 Continuing Studies	Signature	Date
Surinder Aulakh		13/04/22
Chief Information Officer or Privacy Officer	Signature	Date
Associate Director IT	Signature	Date