RENXT Upgrade Privacy Impact Assessment

Project Code	PC0746
Submission Date	July 5, 2017
Organization	University of Victoria
Unit and Service Owner	Advancement Services, Stephanie Rowe Director of Advancement Services
Contact	Greg Churchill, Information Technology Manager, Advancement Services
Reviewed By	[[The CIO or designate responsible for reviewing this PIA. Provide name, title, and contact information]]
Review Date	[[Date of review – can be filled in by PMO or Reviewer]]

1.0 Privacy Context

1.1 Description of Systems and Linkage to Legislation

[[Describe the systems being implemented or changed as a result of this project, and what implications there are in terms of FIPPA.]]

This description and the following sections limit the scope of the PIA to the impact that the changeover to NXT will have.

This project will upgrade the Raiser's Edge system to a SaaS version called Raiser's Edge NXT. The Raiser's Edge system will migrate from UVic to Blackbaud hosting services.

The following Raiser's Edge system components will be changed as a result of this project:

1. Raiser's Edge CRM interface (current state)
    - Desktop application installed on client workstations.
    - Remote application launched from client workstations.
    - Clients use Windows authentication (UVic domain) to sign in.

2. Raiser's Edge remote application server (current state)
    - Clients that do not have the desktop application installed on their workstation access the Raiser's Edge CRM by connecting to the remote application server.
    - Clients use Windows authentication (UVic domain) to sign in.
    - Hosted at UVic.

3. Raiser's Edge database server (current state)
    - All CRM data is stored on the database server.
    - The CRM application connects to the database server.
    - Hosted at UVic.

4. Raiser's Edge web service server (current state)
    - The web services server provides the 'Plug-in Web Service', which allows data to flow between the CRM application and the Sec. 15
    - UVic hosts the Raiser's Edge web services server and Blackbaud hosts the Sec. 15 Sec. 15

The following Raiser's Edge system component changes will occur as a result of this project:

1. Raiser's Edge CRM interface (changed state)
    - Clients access the interface from desktop and mobile devices using a standard web browser.
    - Two web browser versions are available:
        i. NXT web view, which is a mobile-optimized instance of the RENXT service.
        ii. Database view enabled with a Citrix web browser add-on, which is the main, desktop-based instance of the service.
    - Blackbaud hosts the CRM application.
    - Previous desktop applications will be un-installed from client workstations.

2. Raiser's Edge remote application server (changed state)

    - This server is no longer required at UVic and will be decommissioned.

3. Raiser's Edge database server (changed state)
    - All CRM data stored on the database server will be migrated to the new Blackbaud hosting environment.
    - This server is no longer required at UVic and will be decommissioned.

4. Raiser's Edge web service server (changed state)
    - This server is no longer required at UVic and will be decommissioned.

5. Single Sign On (new)
    - Replaces Windows authentication.
    - Clients use the 'Sign in to UVic' service to access the CRM.
    - Single Sign On has three identity management pieces:
        1. i. 'Sign in to UVic' account
            - Format is [UVic client ID]@uvic.ca
            - Provisioned by UVic.
        2. ii. Blackbaud account
            - Linked to the 'Sign in to UVic' account.
            - Contains UVic client ID, first name, last name.
            - Provisioned by Blackbaud.
        3. iii. Raiser's Edge user
            - Linked to the Blackbaud account.
            - Raiser's Edge CRM users belong to the same security group as before upgrade.
            - Provisioned by UVic.
    - Single Sign On service prompts the client for consent to share UVic client ID, first name, last name when provisioning the Blackbaud account. This standard attribute release is performed every time the client signs in. The following language for consent is used for Single Sign On:

      You are about to access the Blackbaud ID sign-in service.
      Information to be provided to this service:
      Full name
      UVic ID
      The information above would be shared with this service if you proceed.
      Do you agree to release this information to the service every time you access it?
      Select an information release consent duration:
      (radio button) Ask me again at next login - I agree to send my information this time.
      (radio button) Ask me again if information changes - I agree that the same information will be sent automatically to this service in the future.
      (button)Decline
      (button)Confirm

The implications of the changes that will be the result of the project in terms of FIPPA are as follows.

FIPPA section 30.1 storage and access must be in Canada:

- All CRM data and personal information stored in the Raiser's Edge database server will be migrated from UVic to data centres hosted by Blackbaud and located in Canada: no implications for FIPPA so long as those Blackbaud's information infrastructure remains in Canada, except as provided for under the consent process described above for Single Sign On system.

- Blackbaud must ensure that personal information in its custody is stored only in Canada and accessed only in Canada: again, no implications so long as the Blackbaud information infrastructure remains in Canada and contractual obligations will be used to ensure that at no point will it be permissible for the contractor to store or access personal information outside of Canada.
- Backup and failover data must also be stored in Canada: again, no implications so long as the Blackbaud information infrastructure remains in Canada and contractual obligations will be used to ensure that at no point will it be permissible for the contractor to store or access personal information outside of Canada.
- Blackbaud staff located in Canada will have administrative access to personal information stored in the systems: FIPPA permits the university's service providers to have restricted access on a need-to-know basis to personal information that the university has collected but that access must be secured against unauthorized collection, use, access, disposal, disclosure, or other interference; accordingly, contractual obligations will be used to ensure that Blackbaud and the university do not make use of unauthorized access to personal information.
- Controls must be in place to ensure that Blackbaud staff located outside of Canada do not have administrative access to personal information stored in these systems: FIPPA does not permit access to personal information from outside of Canada except in accordance with ss. 30.1(by consent or for other permissible purposes), 33.1(1)(e) (for access temporarily from outside Canada), and 33.1(1)(i.1) (for processing payments); accordingly, contractual obligations will be used to ensure that Blackbaud and the university meet their obligations to restrict access to personal information from outside Canada.

For storage and access of personal information outside of Canada, consent will be obtained to authorize that storage and access:

- FIPPA requires that for the operation of the Single Sign On procedures, consent will be obtained clients to share their account information (UVic client ID, first name, last name) with Blackbaud servers in Boston, Massachusetts when provisioning Blackbaud accounts.
- Identity management must implement "attribute release consent" when provisioning a new account and be capable of doing so every time the client signs in.
    - Attribute release consent requires users to accept the release of attributes to service providers during front-channel authentication profiles that include attribute data in the response.

1.2 Use of System

[[Describe what the systems will be used for, how it will be used, who will use it, and how this usage will address FIPPA.]]

This section limits the scope of the PIA to the impact that the changeover to NXT will have.

The Raiser's Edge system is used to perform the same tasks on both the current system and the upgraded system. The significant change is not how the clients use the system but rather how they access the system.

RENXT will be used for the purposes of managing the following:

- Alumni engagement (events, volunteers, academic history, communications);
- Prospective donors (research, ratings, assignment to fundraisers);
- Fundraising activities (identification, cultivation, solicitation, stewardship);
- Sec. 15
-

- Constituent information updates (biographical, contact, relationships, attributes);
- Reports (dashboards, query building, export to excel file);
- Imports (add or update records from an excel file); and
- System administration (user account provisioning, application configuration, database backup).

How RENXT is to be used:

- Clients access the 'NXT web view' using a web browser on a desktop or mobile device;
- Clients access the 'Citrix database view' using a web browser on a desktop; and
- System administrators access a weekly backup file of the Raiser's Edge database from a secure FTP server hosted by Blackbaud.

Who uses RENXT:

- Clients are restricted to approximately Sec. 15 [redacted]
    - Sec. 15 [redacted]
- Two individuals have responsibility for provisioning and de-provisioning accounts:
    - The Information Technology Manager (Advancement Services), and
    - The Data and Applications Coordinator (Advancement Services).
- The "Administrative Systems Access Report" ensures that Raiser's Edge access is appropriate for a user's current job duties. This report is sent to supervisors of staff that have access to the system. Supervisors submit a system access removal request to provision@uvic.ca.

How these uses will be authorized under FIPPA:

FIPPA section 30.1 storage and access must be in Canada:

- The backup file of the Raiser's Edge database is stored on a secure FTP server that is located in Canada and it is intended only to be accessed by UVic clients from within Canada.

'Consent' as referenced throughout FIPPA:

- Single Sign On requires consent from clients to share their account information (UVic client ID, first name, last name) when provisioning the Blackbaud account (data stored in Boston, Massachusetts, USA.)
- Identity management must implement attribute release consent when provisioning a new account and be capable of doing so every time the client signs in.

1.3 Custody and Control

[[Describe what records will be under the possession or use of the institution or system and how the records will be managed to address FIPPA.]]

This section limits the scope of the PIA to the impact that the changeover to NXT will have.

The university will at all times retain control of personal information in RENXT, even where Blackbaud has functional custody over that information. Blackbaud will be retained as a service provider and part of the contractual agreement between the parties will stipulate that the university will retain control of personal information at all times, even if some of that personal information comes into the custody of the university's service providers as they perform authorized functions for the university.

As a result of this project, an exact copy of the current Raiser's Edge database will be made to migrate to the new system. The Raiser's Edge database and the records stored in the database do not change.

The NXT system including the Raiser's Edge database is hosted on the Microsoft Azure platform, which is located in Toronto, Ontario, Canada.

The migration of the Raiser's Edge database to the new system follows these steps:

1. UVic Systems creates a backup file from the current Raiser's Edge production database located at UVic.
2. UVic Systems transfers the database backup file via Sec. 15 at the new Blackbaud hosting environment.
3. Blackbaud restores the backup file to the new Raiser's Edge database server.

New Blackbaud account records are created for Single Sign On clients. These new records will be managed to address 'Consent' as referenced throughout FIPPA:

- Single Sign On requires consent from clients to share their account information (UVic client ID, first name, last name) when provisioning the Blackbaud account (data stored in Boston, Massachusetts, USA.)
- Identity management must implement attribute release consent when provisioning a new account and be capable of doing so every time the client signs in.

1.4 Personally identifiable information Data Types and Information Flows

[[Enumerate all personally identifiable information (PII) data types stored in and accessed by the systems, and how these data types will flow in and out of the systems.]]

This section limits the scope of the PIA to the impact that the changeover to NXT will have.

The first RE NXT *network diagram* provides context to the PII data types and corresponding *data flow diagrams* that follow.

RE NXT Network diagram (Microsoft Azure platform)

Page 67 redacted for the following reason:
- -
Sec. 15

Sec. 15

[redacted]

Blackbaud Payment Service – data flow diagram 2

Sec. 15

[redacted]

Single Sign On – data flow diagram 3

Sec. 15

[redacted]

Sec. 15

The Raiser's Edge database backup file contains the following PII data types:

1. Full name
2. Home address
3. Email address
4. Phone number
5. Personal web address
6. UVic constituent ID
7. Date of birth
8. Ethnicity
9. Gender
10. Relationships to family
11. Academic history
12. Employer and job position
13. Volunteer activity
14. Event attendance
15. Sec. 15
16.
17.
18.

2.0 Privacy Threshold Analysis

[[The purpose of these questions is to help determine what level of privacy and security risk is present in your project. Seek assistance from the PMO if you have any questions. When referencing UVic or external documentation, note the date that the documentation was accessed or provide a copy at the time of reference as an Appendix.]]

1	**Has a Privacy Impact Assessment ever been performed for this project or program?**	**[N] [Date]**
2	**What is the information classification level of information collected, maintained, or shared in any identifiable form as part of this project or service? Select all classification levels that apply.** **See University Policy IM7800 for detailed definitions.** ☒Highly Confidential ☒Confidential ☒Internal ☐Public ☐Don't Know ☐Information is not collected, maintained, or shared in any identifiable form as part of this project or service	
3	**What are the type(s) of personal, critical, or sensitive information collected, maintained, or shared by this project? Please be specific about the data elements.** *Examples include, but are not limited to information about students, employees, donors, alumni, credit cards, health Information, etc. See Appendix A of University Policy IM7800 for more examples.*	

Highly Confidential	• Sec. 15
Confidential	• Personal, academic, employment, activity and business information about students, employees, donors, alumni.
Internal	• FOAPAL codes
Don't Know	•

4	**Does this project or program involve the implementation of a new electronic system or use of a new application/ software to support the creation, collection, storing, backing-up or disposition of personal, sensitive, or critical information?**	**[New]**
5	**Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?** Sec. 15	**[Y]**
6	**Will the project involve the collection or creation of new information about individuals?** • Sec. 15 • Personal, academic, employment, activity and business information about students, employees, donors, alumni.	**[Y/N]**
7	**Will personal information about individuals or sensitive/critical information be disclosed to organizations, programs, processes or people who have not previously had routine access to the information?** Data will be hosted by Blackbaud and therefore would have access.	**[Y]**
8	**Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?** [[If so, how?]]	**[N]**

9	**Will the project collect, use, or disclose PII or sensitive/critical information for research purposes?** [[If so, do you have appropriate research approvals (e.g. ethics)?]]	[N]
10	**Will the project require that individuals are contacted in ways that they may perceive to be intrusive?** [[If so, how may they perceive it to be intrusive?]]	[N]
11	**Is any of the information owned by another organization?** [[If so, which organization(s)?]]	[N]
12	**Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?** [[If so, which ones?]]	[N]
13	**Does this project collect, access or use Social Insurance Numbers (SIN)?**	[N]
14	**How many user records containing PII or sensitive/critical information will be stored, accessed or used?** Sec. 15	Sec. 15
15	**Where will the information be stored?** Blackbaud hosting services in Canada, including failover and backup solutions.	
16	**Will a third party (e.g. vendor or service provider) have access to the information?** Blackbaud.	[Y]
17	**Is any of the information being accessed from outside of Canada?**	[N]
18	**Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems?** Banner student degree information, address, phone, and email information is imported into the Raiser's Edge database from time to time.	[Y]

19	**If there is external sharing, is it pursuant to new or existing information sharing agreements?** [[List these agreements]]	**[New (contract with BlackBaud)]**

3.0 Privacy & Security Risks

[[Based on the sections 1.0 and 2.0, determine the probability, impact, and resulting risk score for each of the following risks. Cite the appropriate privacy and security controls from Appendix A and B in your Risk Mitigation Measures and add to the Response section as appropriate. Probability and impact are rated on a scale of 1-5, with 1 representing a small probability or impact and 5 representing a large probability or impact.]]

ID	Risk Description	Probability (1-5)	Impact (1-5)	Risk Mitigation Measures (reduce probability and/or impact)
1	Lack of legal authority to collection, use or disclose PII	1	4	Privacy controls: AP-1 Authority to Collect AP-2 Purpose Specification
2	Unauthorized collection of PII by authorized individuals/processes/systems	1	3	Privacy controls: IP-1 Consent Security controls: AC-2 Account Management
3	Excessive collection of PII by authorized individuals/processes/systems	1	2	Privacy controls: DM-1 Minimization of Personally Identifiable Information
4	Inappropriate or unauthorized use of PII by authorized individuals/processes/systems	1	2	Privacy controls: UL-1 Internal Use Security controls: AC-2 Account Management AC-8 System Use Notification AC-19 Access Control for Mobile Devices AT-2 Security Awareness Training AU-6 Audit Review, Analysis, and Reporting CM-10 Software Usage Restrictions IA-2 Identification and Authentication (organizational Users)
5	Unauthorized disclosure by individuals/processes/systems	1	4	Privacy controls: UL-2 Information Sharing with Third Parties Security controls: SC-8 Transmission Confidentially and Integrity

6	Creation of new PII by data matching	2	1	Privacy controls: SE-1 Inventory of Personally Identifiable Information
7	Unauthorized tracking of individuals through transaction monitoring	1	3	Privacy controls: AP-1 Authority to Collect AP-2 Purpose Specification SE-1 Inventory of Personally Identifiable Information Security controls: AC-3 Access Enforcement AC-4 Information Flow Enforcement AU-6 Audit Review, Analysis, and Reporting
8	Data stored outside of Canada and in the public cloud	2	2	Privacy controls: IP-1 Consent Security controls: AC-3 Access Enforcement AC-4 Information Flow Enforcement AC-22 Publically Accessible Content CM-8 Information System Component Inventory SC-7 Boundary Protection
9	Data retention beyond prescribed timeline	1	2	Privacy controls: DM-2 Data Retention and Disposal Security controls: CM-9 Information System Backup SI-12 Information Handling and Retention
10	Risk of increased surveillance	2	3	Security controls: AC-3 Access Enforcement AC-4 Information Flow Enforcement AC-22 Publically Accessible Content AU-6 Audit Review, Analysis, and Reporting SC-7 Boundary Protection SC-8 Transmission Confidentially and Integrity
11	Unauthorized use as a records repository	1	1	Privacy controls: DM-2 Data Retention and Disposal Security controls: CM-10 Software Usage Restrictions

				SI-12 Information Handling and Retention
12	Public perception	2	3	Privacy controls: IP-1 Consent IP-2 Individual Access IP-3 Redress IP-4 Complaint Management Security Controls: SI-8 SPAM Protection
13	Use of existing PII data in a new system or business process	2	1	Privacy controls: AP-2 Purpose Specification AU-6 Audit Review, Analysis, and Reporting Security controls: AC-19 Access Control for Mobile Devices AC-20 Use of External Information Systems

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

Service Area	Impact? (Y/N)	Leader	Expert Consulted	Date of Consultation
Office of the CIO		Wency Lum		
Systems General Office		Chandra Beaveridge		9/6/2017
Client Technologies		Lance Grant		9/6/2017
Desktop Support Services		David Street		9/6/2017
Computer Help Desk		Marcus Greenshields		9/6/2017
Academic & Admin Services		Nav Bassi		9/6/2017
Client Account Managers		Garry Sagert		9/6/2017
Production and Technical Support		Rizwan Bashir		9/6/2017
Development Services		Scott Thompson		23/5/2017
Identity Services		Corey Scholefield		9/6/2017
UVic Online		Garry Sagert		9/6/2017
Data Centre Services		Kim Lewall		9/6/2017
Network Services		Jane Godfrey		9/6/2017
Infrastructure Services		Ron Kozsan		9/6/2017
Information Security Office		Lance Grant		9/6/2017
Project Management Office		Chandra Beaveridge		9/6/2017

Sponsor

The project sponsor or system owner must be consulted in the creation of the Privacy Impact Assessment. Use this table to document consultation with the project sponsor or service owner.

Name	Comments	Date of Consultation
Stephanie Rowe		9/6/2017

Other Projects

[[Please include a table like the above for any other subject matter experts that you believe should provide input for this PIA.]]

Department/Unit	Leader	Expert Consulted	Date of Consultation

Revision History

[[As the PIA is distributed between the sponsor, stakeholders, and SMEs, update this table to indicate changes between document versions.]]

Version	Date	Author	Comments
1	30/6/2017	Greg Churchill	Completed section 1
2	4/7/2017	Greg Churchill	Appended additional data flow diagrams to section 1.4; Completed section 2;

			Need expert advice on section 3
2.1	5/7/2017	Greg Churchill	Updated section 1.2, identifying provision staff and process; Updated section 1.3, specifying Azure platform and describing migration data flow.
2.2	6/7/2017	Greg Churchill	Added attribute release consent language; staff descriptions; other changes as requested by Rowan Hodge.

Appendix A – Privacy Controls

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	**Authority to Collect** The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need. **Response:** GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00
AP-2	**Purpose Specification** The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00
DM	Data Minimization and Retention
DM-1	**Minimization of Personally Identifiable Information** Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 19.00
DM-2	**Data Retention and Disposal** Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records). **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 20.00, 25.00
DM-3	**Minimization of PII Used in Testing, Training, and Research** Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and Implements controls to protect PII used for testing, training, and research **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 20.00, 21.00, 22.00
IP	**Individual Participation and Redress**

ID	PRIVACY CONTROLS
IP-1	**Consent** Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 18.00
IP-2	**Individual Access** Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 29.00, 32.00
IP-3	**Redress** Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 30.00, 31.00, 33.00
IP-4	**Complaint Management** The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 34.00
SE	**Security**
SE-1	**Inventory of Personally Identifiable Information** Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

ID	PRIVACY CONTROLS
SE-2	**Privacy Incident Response** Develops and implements a Privacy Incident Response Plan; and Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, Procedures for responding to a Privacy Incident or Privacy Breach
UL	**Use Limitation**
UL-1	**Internal Use** The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00
UL-2	**Information Sharing with Third Parties** Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. **Control(s) / Compliance:** GV0235 Protection of Privacy Policy, section(s) 17.00, 20.00, 21.00, 22.00m 23.00, 24.00, 31.00,

Appendix B – Security Controls

ID	SECURITY CONTROLS
AC-2	**Account Management** **Control:** • Identifies and selects the following types of information system accounts to support organizational missions/business functions: organization-defined information system account types; • Assigns account managers for information system accounts; • Establishes conditions for group and role membership; • Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; • Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; • Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions; • Monitors the use of information system accounts; • Notifies account managers: • When accounts are no longer required; • When users are terminated or transferred; and • When individual information system usage or need-to-know changes; • Authorizes access to the information system based on: • A valid access authorization; • Intended system usage; and • Other attributes as required by the organization or associated missions/business functions; • Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and • Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. **Response:** • Account Management is governed by the following institutional policies and procedures: • IM7200 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf • Account Management is subject to the operating procedures and processes of the University. [[Add additional relevant information as required.]]
AC-3	**Access Enforcement** **Control:** • The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies. **Response:** • See AC-4, SC-7 [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS
AC-4	**Information Flow Enforcement** **Control:** The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on organization-defined information flow control policies. **Response:** • See SC-7 [[Add additional relevant information as required.]]
AC-8	**System Use Notification** **Control:** Displays to users an organization-defined system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. **Response:** • Organization-defined systems use policy will: • Primarily positive and explanatory (and not just a list of "don'ts"). • Encourage usage by providing positive examples and suggestions. • Require that content be office-appropriate. • Require that personally identifiable information is not used. • Include links to University of Victoria policies and training resources • Organization-defined systems use policy will include reference to and compliance with: • IM700 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf • GV0235 – Protection of Privacy http://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf • IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf • Canadian Copyright Act http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-42/latest/rsc-1985-c-c-42.html [[Add additional relevant information as required.]]
AC-19	**Access Control for Mobile Devices** **Control:** • Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and • Authorizes the connection of mobile devices to organizational information systems **Response:** • University of Victoria recommends for all users and requires for Exchange users the use of: Sec. 15 [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS
AC-20	**Use of External Information Systems** **Control:** - The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: - Access the information system from external information systems; and - Process, store, or transmit organization-controlled information using external information systems. **Response:** - See CP-9, PE-3, SC-7, SI-8 [[Add additional relevant information as required.]]
AC-21	**Information Sharing** **Control:** The organization: - Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for organization-defined information sharing circumstances where user discretion is required and - Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. **Response:** - See AC-20 [[Add additional relevant information as required.]]
AC-22	**Publically Accessible Content** **Control:** The organization: - Designates individuals authorized to post information onto a publicly accessible information system; - Trains authorized individuals to ensure that publicly accessible information dees not contain nonpublic information; - Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and - Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered. **Response:** - See AC-4, AC-21, IA-2, IA-8 [[Add additional relevant information as required.]]
AT-2	**Security Awareness Training** **Control:** - The organization provides basic security awareness training to information system users (including managers, senior executives, and confractors): - As part of initial training for new users; - When required by information system changes; and

ID	SECURITY CONTROLS
	• Organization-defined frequency thereafter. **Response:** • Privacy training will be required for new users to ensure compliance with FIPPA. [[Add additional relevant information as required.]]
AU-6	**Audit Review, Analysis, and Reporting** **Control:** The organization: • Reviews and analyzes information system audit records for indications of defined inappropriate or unusual activity. • Reports findings to the Chief Privacy Officer and Chief Information Officer **Response:** [[Add additional relevant information as required.]]
CA-3	**System Interconnections** **Control:** The organization: • Authorizes connections from the information system to other information systems through the use of interconnection Security Agreements; • Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and • Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]. **Response:** [[Add additional relevant information as required.]]
CM-3	**Configuration Change Control** **Control:** The organization: • Determines the types of changes to the information system that are configuration-controlled; • Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; • Documents configuration change decisions associated with the information system; • Implements approved configuration-controlled changes to the information system; • Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period]; • Audits and reviews activities associated with configuration-controlled changes to the information system; and • Coordinates and provides oversight for configuration change control activities through the: organization-defined configuration change control that convenes organization-defined configuration change conditions. **Response:** • System configuration settings and changes are managed using the University systems Change Management processes and Change Advisory Board (CAB). [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS
CM-8	**Information System Component Inventory** **Control:** • Develops and documents an inventory of information system components that: • Accurately reflects the current information system; • Includes all components within the authorization boundary of the information system; • Is at the level of granularity deemed necessary for tracking and reporting; and • Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and • Reviews and updates the information system component inventory. **Response:** [[Add additional relevant information as required.]]
CM-10	**Software Usage Restrictions** **Control:** The organization: • Uses software and associated documentation in accordance with contract agreements and copyright laws; • Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and • Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. **Response:** [[Add additional relevant information as required.]]
CP-2	**Contingency Plan** **Control:** The organization develops a contingency plan for the information system. **Response:** [[Add additional relevant information as required.]]
CP-9	**Information System Backup** **Control:** Conducts backups of user-level information contained in the information system. Conducts backups of system-level information contained in the information system. Conducts backups of information system documentation including security-related documentation; and Protects the confidentiality, integrity, and availability of backup information at storage locations. **Response:** [[Add additional relevant information as required.]]
IA-2	**Identification and Authentication (organizational Users)** **Control:** • The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

ID	SECURITY CONTROLS
	Response: • See SC-8 [[Add additional relevant information as required.]]
IA-8	**Identification and Authentication (non-organizational users)** **Control:** • The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). **Response:** • See SC-8 [[Add additional relevant information as required.]]
MP-2	**Media Access** **Control:** • The organization restricts access to organization-defined types of digital and/or non-digital media] to personnel or roles. **Response:** [[Add additional relevant information as required.]]
PE-3	**Physical Access Control** **Control:** • Enforces physical access authorizations, controls and audits exist. **Response:** [[Add additional relevant information as required.]]
PL-4	**Rules of Behavior** **Control:** • Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; • Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system; • Reviews and updates the rules of behavior; and • Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated **Response:** • See AC-8, CM-10 [[Add additional relevant information as required.]]

ID	SECURITY CONTROLS
RA-3	**Risk Assessment** **Control:** The organization: • Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; • Reviews risk assessment results [Assignment: organization-defined frequency]; • Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and • Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. **Response:** • See sections 1.4 and 3.0 of this document. [[Add additional relevant information as required.]]
SC-7	**Boundary Protection** **Control:** • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; • Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. **Response:** [[Add additional relevant information as required.]]
SC-8	**Transmission Confidentially and Integrity** **Control:** • The information system protects the confidentiality and; integrity of transmitted information. **Response:** [[Add additional relevant information as required.]]
SI-8	**SPAM Protection** **Control:** The organization: • Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and • Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures **Response:** [[Add additional relevant information as required.]]
SI-12	**Information Handling and Retention** **Control:**

ID	SECURITY CONTROLS
	• The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements **Response:** • Use policy states that all users must comply with IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf [[Add additional relevant information as required.]]