Counselling Services - PrivacEmail Privacy Impact Assessment

Project Code	PC 0762
Submission Date	[[Date of submission – can be filled in by PMO]]
Organization	University of Victoria
Unit and Service Owner	Counselling Services
Contact	Lawrence Murphy, Therapy Online, email: research@sympatico.ca Ai-Lan Chia, Associate Director, Counselling Services, achia@uvic.ca
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.]]

Counselling Services at UVic are looking into ways to offer counselling to currently enrolled and degree-seeking UVic students who can access counselling via an online platform, without the requirement to be physically present at Counselling Services location. Students can choose to access counselling on site via face-to-face session with a counsellor at Counselling Services, and can also choose to access counselling via distance through this platform (i.e., PrivacEmail system). This system will allow text-based counselling session when student clients exchange written text with counsellors (real-time or non-synchronized exchange of text).

The aforementioned online platform (i.e., PrivacEmail system), via the vendor "Worldwide Online Therapy", is a secure encrypted web-based service where information is collected and stored in an encrypted database. The underlying architecture is a CMS that allows for different roles and different levels of permissions. The PrivacEmail system is a cloud based solution hosted within Canada with storage in a Canadian data centre (called Sec. 15 Worldwide Online Therapy has a contractual arrangement with the company Sec. 15 who handles technical support to the PrivacEmail system (e.g., program or software development and updates; file deletion which is to be further explained later in this document). Worldwide Online Therapy has another contractual relationship with a website technician who manages website management.

In accordance with FIPPA section 26 (h), the purpose for collection of the information is in alignment with legislation to provide a service.

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.]]

The PrivacEmail system will allow UVic students to access services available at Counselling Services from distance, which increases service accessibilities especially for students who are in distance academic program, are in coop full work term full-time, are mobility-challenged, or are simply very busy with various life and academic commitments. The service providers are the existing counselling team at Counselling Services (no contractual arrangement needed with any non UVic/outside service provider to provide counselling). Several counsellors at Counselling Services team have already completed necessary professional development training to offer text based counselling sessions.

Sec. 15 the existing client file record management system used by Counselling Services, continues to be the primary holder for any documentation related to counselling sessions including necessary forms and session notes for in person and distance sessions.

For text-based distance counselling sessions, Counselling Services will make prior arrangement with the students to gather consent and intake information (using Counselling Services Consent Form and Counselling Services Intake Form); note that all students accessing Counselling Services will complete these two forms. For text based counselling, prior arrangement will be made to gather additional consent (using Counselling Services Distance Counselling Consent Form; to be drafted) and to provide PrivacEmail usage information such as how to create a user account (Counselling Services Distance Counselling Client Information Sheet; to be drafted) in order to

adequately prepare students to use the system. These forms are built into therefore stored within Sec. 15 as the rest of client files.

Counsellors at the Counselling Services team are to create their own individual account at the PrivacEmail system, similar to that each client has their own unique account. Information required to create an account in the PrivacEmail system includes a first and last name and an email address. Counsellors log in at their personal workstation on site at Counselling Services during their work hours (therefore no remote, mobile, or outside-work-hour access). In addition to each counsellor's account, Counselling Services will create a clinical administrative account that is used to 1) provide helpdesk-like administrative support to clients and counsellors if needed to, e.g., resetting password, to 2) manually assign a particular client's account to a specific counsellor's account for them to engage counselling session within PrivacEmail system, and to 3) coordinate between Counselling Services and Worldwide Therapy Online staff (e.g., coordinate routine system upgrades; identify and report possible threats of privacy breach to Associate Director/ Director of Counselling Services). Client authentication is determined by the clinical administrative account holder who is to review client account registration information in PrivacEmail system and review client file information in Sec. 15 contact the account holder within PrivacEmail to obtain additional authentication information (i.e., V number; date of birth) and compare the key identifier information (e.g., V number; date of birth) to conclude these two accounts being held by the same individual. Once it is confirmed the specific account holder being the same student requesting text based counselling, then the clinical administrative account holder will assign the student with their respective counsellor who then will begin text based counselling sessions.

In accordance with FIPPA section 33.1, consent to release personal information is collected from the client at the time when the client agrees to receive text based counselling during the intake session at the Counselling Services centre and before the client creates an account in the system. The client will be reminded for the content of the consent after they log in to create an account.

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.]]

The PrivacEmail system contains client account registration information (i.e., first and last name; email address), client authentication related text communications between client and clinical/administrative account holder, and counselling session related text communications between counsellors and clients. Records within the PrivacEmail system are held on secure servers located in Canada in an encrypted database (i.e., Sec. 15 Sec. 15 . When a client or a counsellor logs into the PrivacEmail system, they are logging into the Sec. 15 All communication takes place on the servers (therefore no data transmission from the PrivacEmail system to the server and vice versa). After distance sessions occurring within the PrivacEmail system, counsellors are to manually enter session note directly into the client's file in Sec. 15 Information gathered by Sec. 15 s not subject to this Privacy Impact Assessment and all client information is collected and stored within the existing Sec. 15

In accordance with FIPPA sections 27 through 29, students provide their information directly, can review and correct the accuracy of the information collected.

Record management practices for records within the PrivacEmail system are to follow the principles laid out for record management of Sec. 15 That is, each client has a specific file (with a file number). Record retention is seven years after the last contact with the student, plus the years of majority. Sec. 15 has various level of permission for file accesses (e.g., those with clinical director having access to all files; those as counsellors having access to their own clients). Please note again that data within Sec. 15 is not subject to this Privacy Impact Assessment. For files within PrivacEmail, the clinical administrative account holder from

Counselling Services is to assign a client to his/her counsellor who has his/her own PrivaEmail account; thus, counsellors only have access to the files of their own clients within PrivacEmail system. For file retention and disposition, clinical administrative account holder is to contact Worldwide Therapy Online staff (who only have access to file numbers and account registration information, not counselling text-content), by providing them a list of file number whose files fulfill file disposition criteria and then asking those files deleted permanently. Worldwide Therapy Online staff is to contact Sec. 15 by providing them a list of file numbers to delete files from Sec. 15 Note that UVic client file data is segregated in Sec. 15 from other data the Sec. 15 hosts. Worldwide Therapy Online staff is then to provide a confirmation to the clinical administrative account holder regarding the completion of file disposition.

UVic's data retention policy for Counselling records:

Student Services SS085-20 Counselling case files

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.]]

The PrivacEmail system is a closed system. Any and all data can only be retrieved through the PrivacEmail system itself.

The PrivacEmail system holds student/client account registration information (as aforementioned). Counselling Services will arrange one staff member being the holder of the clinical administrative account to the PrivacyEmail system to review account registration information and assign student to a counsellor. Students will log into the system directly and engage text-based counselling session with their assigned counsellor. When offering text-based counselling sessions, counsellors will respond to text written by student clients. Details of the counselling sessions will be summarized by the counsellor offering the session and entered directly into the Sec. 15

No data will be automatically transmitted between systems Sec. 15 and PrivacEmail systems. As noted above, all contacts within PrivacEmail system take place on the servers (therefore no data transmission from the PrivacEmail system to the server and vice versa).

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** • Student/client account registration information (first and last name, email address) and client authentication text based exchange between client and admin clinical counsellor (V number; date of birth). **Internal** • **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? [[If so, what are those technologies? - Sec. 15 Examples include, but are not limited to, cloud platforms (SaaS, PaaS, IaaS), social media, mobile applications, smart cards, RFID, biometrics, locator technologies, visual surveillance, video recording, profiling, data mining, etc.)]]	[Y]
6	Will the project involve the collection or creation of new information about individuals? [[If so, what information?]] Clients will disclose personal and confidential information in communications with counsellors.	[Y]
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? [[If so, which organizations, processes or people?]]	[N]
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? Note that it is intended to be included in the contractual language that Worldwide Online Therapy will not use UVic data for research or other use of information. [[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? [1-1000],[1001-5000],[5,001-50,000],[50,001-100,000],[100,000+]	Sec. 15
15	Where will the information be stored? Provider within Canada Sec. 15	
16	Will a third party (e.g. vendor or service provider) have access to the information? [[If so, which third parties?]] Worldwide Therapy Online Staff and its two specific contractors (i.e Sec. 15 one website technician) will have access to the account registration information (i.e., student's name, email address).	[Y]
17	Is any of the information being accessed from outside of Canada? [[If so, by whom and from where?]]	[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? The PrivacEmail system is a closed system with no connections to other systems, including outside email services.	[N]
19	If there is external sharing, is it pursuant to new or existing information sharing agreements? n/a	[n/a]

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	1	Accept. Legal authority to collect personal information is provided by the University Act.
2	Unauthorized collection of PII by authorized individuals/processes/systems	1	1	Accept. All direct data entry into this system will be made by clients and their counsellors.
3	Excessive collection of PII by authorized individuals/processes/systems	1	1	Accept. All direct data entry into this system will be made by clients and their counsellors.
4	Inappropriate or unauthorized use of PII by authorized individuals/processes/systems	1	1	Accept. All data access in the system will be a direct result of client/counsellor communications and following the completion of the forms for consent for use/release of information
5	Unauthorized disclosure by individuals/processes/systems	1	1	Mitigate. The PrivacEmail system is a closed system with access limited to Sec. 15 UVic Counselling Services team. Client information is only accessible to the client and UVic Counselling Services team.
6	Creation of new PII by data matching	1	1	Mitigate. The PrivacEmail system is a closed system.
7	Unauthorized tracking of individuals through transaction monitoring	1	1	Mitigate. The PrivacEmail system is a closed system.
8	Data stored outside of Canada and in the public cloud	1	1	Mitigate. The PrivacEmail system is a cloud based system hosted at a Canadian storage location.
9	Data retention beyond prescribed timeline	1	2	Mitigate. Counselling services will apply the UVic data retention policies and will request the vendor to delete records that are encrypted via file number and are no longer required. The vendor is responsible to completing the deletion request. UVic will request verification from the vendor for the list of deleted file numbers.
10	Risk of increased surveillance	1	2	Mitigate. The PrivacEmail system is a cloud based system hosted at a Canadian storage location.
11	Unauthorized use as a records repository	1	1	Accept. The PrivacEmail system holds text based personal and confidential exchange between student and their counsellor.

12	**Public perception**	2	2	**Mitigate. Counselling Services will communicate the benefits and risks of the PrivacEmail system using the department website. The public will be informed and the department use of the system will be transparent for all clients. A new client consent form for use of the PrivacEmail system will be created, used and stored within Counselling Services** Sec. 15 **A client information sheet that is to be drafted for the project, outlining safeguards and potential risks, will be provided to each client who consents to receive text based counselling.**
13	**Use of existing PII data in a new system or business process**	3	3	**Accept. The PrivacEmail system is intended to provide text based counselling services for clients who have gone through intake session at the Counselling Services prior.**

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		
Client Technologies		Lance Grant		
Desktop Support Services		David Street		
Computer Help Desk		Marcus Greenshields		
Academic & Admin Services		Nav Bassi		
Client Account Managers		Garry Sagert		
Production and Technical Support		Rizwan Bashir		
Development Services	Y	Scott Thompson		
Identity Services		Corey Scholefield		
UVic Online		Garry Sagert		
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Infrastructure Services		Ron Kozsan		
Information Security Office		Lance Grant		
Project Management Office		Chandra Beaveridge		

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
Ai-Lan Chia		14-Aug-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
0.1	14 August 2017	Tracey MacNeil Ai-Lan Chia	Initial draft

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,

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.]]