Ellucian Mobile Implementation Privacy Impact Assessment

Project Code	PC0597
Submission Date	[[Date of submission – can be filled in by PMO]]
Organization	University of Victoria
Unit and Service Owner	Garry Sagert, UVic Online
Contact	Rizwan Bashir, Team Lead/Senior Programmer Analyst, 721-8869
Reviewed By	Garry Sagert, Director, UVic Online, 721-7692
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

We intend to replace the current UVic mobile app with Ellucian Mobile, which is a higher education mobile app that easily integrates with Banner, University of Victoria's mission critical administrative system. Please note that students' use of this mobile app is optional, and that all personally identifiable information is exchanged directly between the student's mobile device and UVic servers, without involving third party services other than networking. Any student functionality provided in the mobile app is available via student self-service.

The main components of Ellucian Mobile are:

1) Mobile app: This is user's mobile device i.e. IPhone, IPad
2) Mobile Integration server: This is a Linux server residing Sec. 15
3) Mobile database server: This is a Linux server residing in
4) Mobile Configuration Web Application: The Configuration web application is a web tool that allows University Systems to set up and manage UVic Mobile configurations, which are forwarded to the student's mobile device so it can contact UVic servers directly. This web application is hosted Sec. 15 Sec. 15 No personally identifiable information is entered into this web application.

Mobile Integration Server

The Mobile Integration Server is a web services app that handles all communication between the mobile devices and the UVic Student Information system. For example, the Mobile Server does the following:

1) Authenticates students against Sec. 15 when students sign into the app.
2) Retrieves and displays the financial information, student's grades and course information from Sec. 15 Sec. 15 on the student's mobile device.

1.2 Use of System

<u>What the system will be used for?</u>

Upgraded UVic mobile app will allow (but not require) UVic students to:

1) View their final grades
2) View their class schedule
3) View and add funds to their ONECard balance

Upgraded UVic mobile app will allow public to:

1) View transit information (NextBus)
2) View security and emergency information
3) View campus dining information
4) View campus news feed

<u>Who will use it?</u>

Upgraded UVic mobile app will be used by:

1) University of Victoria Students
2) Public

FOI2024-017 - 2016

How will it be used?

Users will download UVic mobile app from app stores, such as iTunes and Google Play. When users open the application for the first time, the mobile device will connect to the Mobile configuration Web Application. This Web Application will send the following configuration definitions to the user's device:

1) The color scheme
2) Home screen images
3) The list of available modules

Once the user begins interacting with the application, all requests are handled directly through Sec. 15 Sec. 15 which resides in Sec. 15 Information will flow between Sec. 15 and Sec. 15 which is a protocol for secure communication and ensures protection of the privacy and integrity of data.

The actual data sent to the user **does not** pass through the Sec. 15 The information stored in the Web Configuration tool is limited to the following:

1) Configuration identifiers
2) Branding Information (colors, icons and images)
3) Definitions of modules setup by University Systems

Sensitive information that enables mobile devices to communicate with Sec. 15 is stored in the Sec. 15 which resides in Sec. 15

1.3 Custody and Control

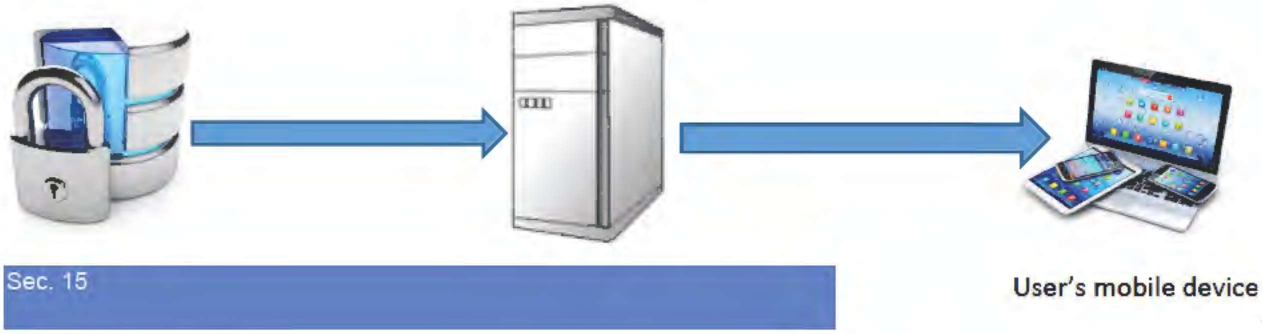
When students add funds to their ONECard account using their mobile device, that information will be stored in Sec. 15 which is hosted in Sec. 15 Please note that functionality to view and add funds to ONECard already exists and is available via Student Self Service web.

Students grades, student schedule and student financial information exists in Sec. 15 and this data will flow from Sec. 15 to user's mobile device and NOT vice versa.

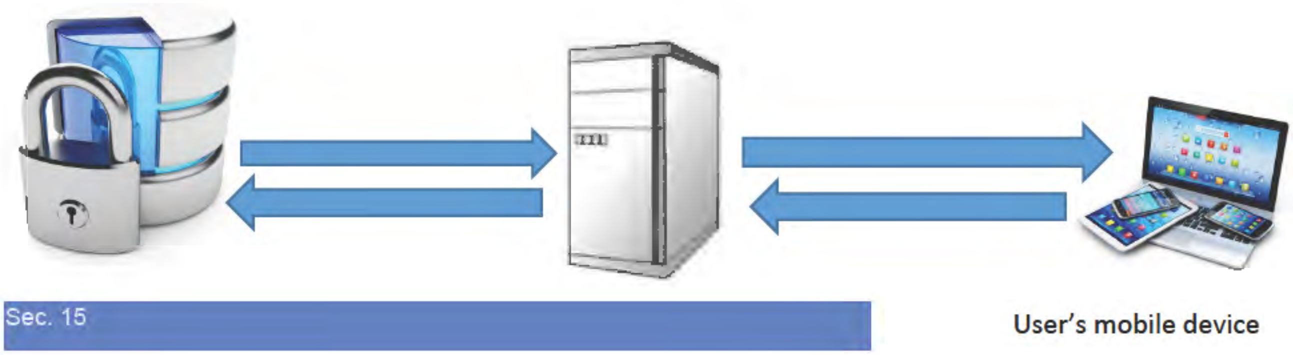
Mobile Sec. 15 does not store any confidential information.

1.4 Personally identifiable information Data Types and Information Flows

1) Student financial information
   a. Recent payments
   b. Current balance
   c. ONECard balance
2) Student class schedule
3) Student grades



4) Student registration and ONECard data will both ways:



FOI2024-017 - 2016

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.]]

<table>
<tr><td><b>1</b></td><td><b>Has a Privacy Impact Assessment ever been performed for this project or program?</b></td><td><b>No</b></td></tr>
<tr><td><b>2</b></td><td colspan="2"><b>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.</b>
<b>See University Policy IM7800 for detailed definitions.</b>
☐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</td></tr>
<tr><td><b>3</b></td><td colspan="2"><b>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.</b>

<i>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.</i>
<table>
<tr><td><b>Highly Confidential</b></td><td>•</td></tr>
<tr><td><b>Confidential</b></td><td>• Student grades, Student class schedule, financial information and ONECard balance</td></tr>
<tr><td><b>Internal</b></td><td>•</td></tr>
<tr><td><b>Don't Know</b></td><td>•</td></tr>
</table></td></tr>
<tr><td><b>4</b></td><td><b>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?</b></td><td><b>This project provides an additional means for students to interact with UVic; however it does not add any new services.</b></td></tr>
<tr><td><b>5</b></td><td><b>Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?</b>

This project will create the ability for students to view confidential student information and register for courses on their mobile devices via a UVic-sanctioned app. However usage is optional.</td><td><b>Yes</b></td></tr>
<tr><td><b>6</b></td><td><b>Will the project involve the collection or creation of new information about individuals?</b>

[[If so, what information?]]</td><td><b>No</b></td></tr>
<tr><td><b>7</b></td><td><b>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?</b>

[[If so, which organizations, processes or people?]]</td><td><b>No</b></td></tr>
<tr><td><b>8</b></td><td><b>Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?</b></td><td><b>Yes</b></td></tr>
</table>

	We are providing students a new way to view their class schedule, student grades and ONECard balance via a UVic-sanctioned app. However usage is optional	
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)?]]	**No**
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?]]	**No**
11	**Is any of the information owned by another organization?** [[If so, which organization(s)?]]	**No**
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?]]	**No**
13	**Does this project collect, access or use Social Insurance Numbers (SIN)?**	**No**
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?** Data will be stored in the UVic data centre. Mobile applications are downloaded from the App Store and Google Play, and contact servers in the UVic data centre for configuration information and connectivity with UVic systems. Device UDCID may be stored in the Ellucian configuration web application for faculty, staff and students who wish to enable push notifications via the UVic Mobile app.	
16	**Will a third party (e.g. vendor or service provider) have access to the information?** Ellucian will have access to device UDCID for faculty, staff and students who wish to enable push notifications via the UVic Mobile app.	**Yes**
17	**Is any of the information being accessed from outside of Canada?** Students may choose to access their information while living and/or travelling outside of Canada. Ellucian will have access to device UDCID for faculty, staff and students who wish to enable push notifications via the UVic Mobile app	**Possibly**
18	**Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems?** Personal information is shared between the mobile application and a variety of enterprise information systems at UVic, including but not limited to Banner, ONECard, CAS and possibly CourseSpaces (Moodle).	**Yes**
19	**If there is external sharing, is it pursuant to new or existing information sharing agreements?** [[List these agreements]]	**There is no external information sharing.**

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	N/A	N/A	No new information is being collected or used in UVic Mobile app. All information collected or used in UVic Mobile app is already collected and used via Banner Self Service
2	Excessive collection of PII by authorized individuals/processes/systems	N/A	N/A	
3	Creation of new PII by data matching	N/A	N/A	
4	Data stored outside of Canada and in the public cloud	1	2	No confidential information is stored outside of Canada or in public cloud. Ellucian will store UDCID which is behind their Load Balancer and a firewall
5	Data retention beyond prescribed timeline	N/A	N/A	No new data is being captured via Mobile app. Data retention of grades and registration information does not change with implementation of new mobile app.
6	Risk of increased surveillance	N/A	N/A	Mobile app does not include any surveillance
7	Public perception	1	1	Student registration, grades, schedule, financial information and ONECard information will require students to log into the mobile app with UVic credentials. Students can be assured that this information is only available to them only after they securely log into the app. Camosun college has also implemented the same mobile app in similar manner.

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		Nav Bassi, Ron Kozsan, Garry Sagert		
Systems General Office		Trish Kearley		
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		Scott Thompson	Scott Thompson	
Development Services		Dave Wolowicz	Dave Wolowicz	
Identity Services		Corey Scholefield		
UVic Online		Garry Sagert	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
Garry Sagert		

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
1.0	**Feb 15, 2016**	**Rizwan Bashir**	**Initial draft**

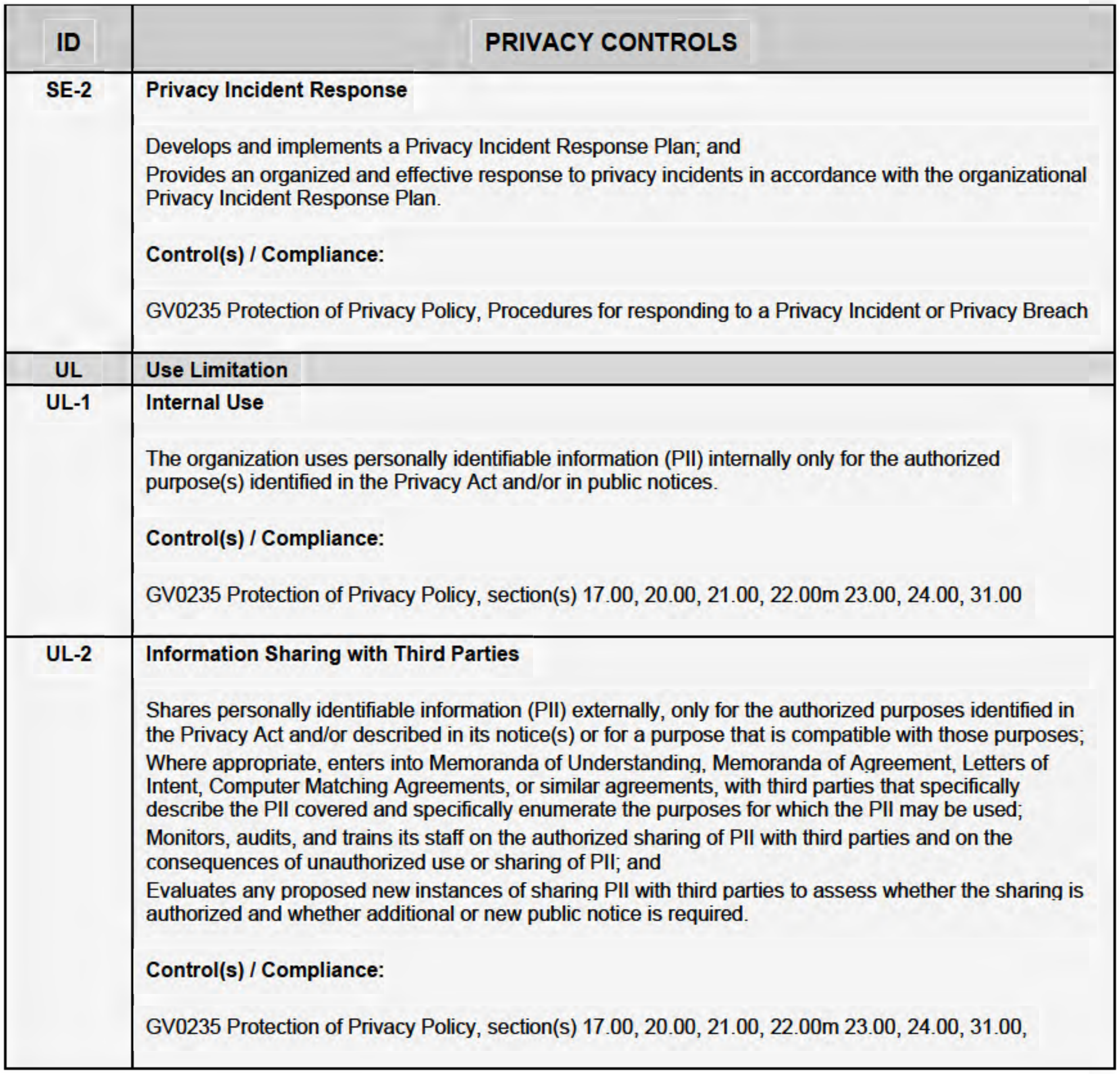
Appendix A – Privacy Controls

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**

FOI2024-017 - 2016

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 descr bed 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.

FOI2024-017 - 2016



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,

FOI2024-017 - 2016

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.]]

FOI2024-017 - 2016

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: - an encrypted mobile device - a password protected mobile device - device wipe on failed login attempts [[Add additional relevant information as required.]]

FOI2024-017 - 2016

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 contractors): - 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]; • Andils 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 distr bution, 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).

FOI2024-017 - 2016

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.]]

FOI2024-017 - 2016

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.]]