University of Victoria

Uvic Vikes Online Tickets Privacy Impact Assessment

Project Code	PC07577
Submission Date	[[Date of submission – can be filled in by PMO]]
Organization	University of Victoria
Unit and Service Owner	UVic Athletics and Recreation Services
Contact	Garry Sagert, Director, UVic Online Tracey MacNeil, Client Account Manager, UVic Online
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.]]

The Uvic Vikes Ticketing management system project seeks to implement ticket management software and hand-held ticket scanning hardware from the vendor University Tickets. The system will become the primary Athletics ticketing and point of sale solution for Vikes Athletics for online and in-person ticket sales, reserve seating in the CARSA performance gymnasium, and ticket scanning for event admissions.

The system will contain client profiles for community patrons and may include personally identifiable information (PII) such as names, addresses, email address, phone numbers and payment information. In addition, client purchasing history will be retained for tracking and loyalty rewarding.

The online software is cloud-based and hosted in the US. As such, all patrons will be informed of the out-of-country storage and be given the opportunity to provide consent when they create their accounts. Those who chose not to provide consent will have the opportunity to purchase tickets in person at the ticket desk, without having their PII entered into University Tickets.

A limited number of complimentary tickets are reserved for students and employees, who can also collect their complimentary tickets at the ticket desk without having their information entered into University Tickets.

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 University Tickets system will be used for the management and sale of event tickets for Vikes Athletics events. Clients will be able to electronically purchase tickets for events, select seats for designated venues, print at home or electronically save and present their ticket at the event. Tickets will be scanned using vendor provided hand held, wireless scanners.

To purchase tickets online for Athletic events, community patrons will create an account in the University Tickets system, enter their personal information (name, address, email address, phone number, and payment information) select their tickets, and pay online.

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

When a community patron creates an account in the system, the information will be stored in a US-based cloud service provider.

In accordance with FIPPA section 33.1, consent to release personal information will be collected from the client at the time the client creates an account in the system.

Community patrons will be asked to confirm consent on the account information page. The consent language will be confirmed by UVic Privacy Office, and will be similar in content to the UBC Consent block:

"I consent to the secure storage of my personal information outside of Canada (in the U.S.A) in accordance with the privacy policy of UniversityTickets outlined in the Privacy Policy. "

A community patron cannot create their account without acknowledging the consent. At this time, there is no additional tracking of the action of the consent.

Students and employees will not normally interact with University Tickets, but instead will collect complimentary tickets at the front desk. Community patrons who do not wish to create an online account will be able to obtain printed tickets in person at the CARSA ticket counter in the same manner as students and employees.

Community patrons will be informed via a privacy disclosure statement that the information is hosted on a US storage location. The UBC implementation of University Tickets provides an example of the privacy policy that will be in place for UVic.

Additional information on the University Tickets solution is available from:

http://www.universitytickets.com/athletic-solutions/

http://www.universitytickets.com/mobile-ticketing/

http://www.universitytickets.com/scanners/

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 records managed by the system will include client profiles for community patrons and may include PII such as names, addresses, email address, phone numbers and payment information. In addition, client purchasing history will be retained for tracking and loyalty rewarding.

The vendor retains client information and does not share with outside parties except for the purposes of completing an order. Email addresses may be used for marketing if a client opts in to be including in the marketing products.

In accordance with FIPPA sections 27 through 29, Clients provide their information directly, can review and correct the accuracy of the information collected. For more information on the University Tickets privacy policy, refer to:

http://www.universitytickets.com/downloads/PrivacyPolicy.pdf

1.4 Personally identifiable information Data Types and Information Flows

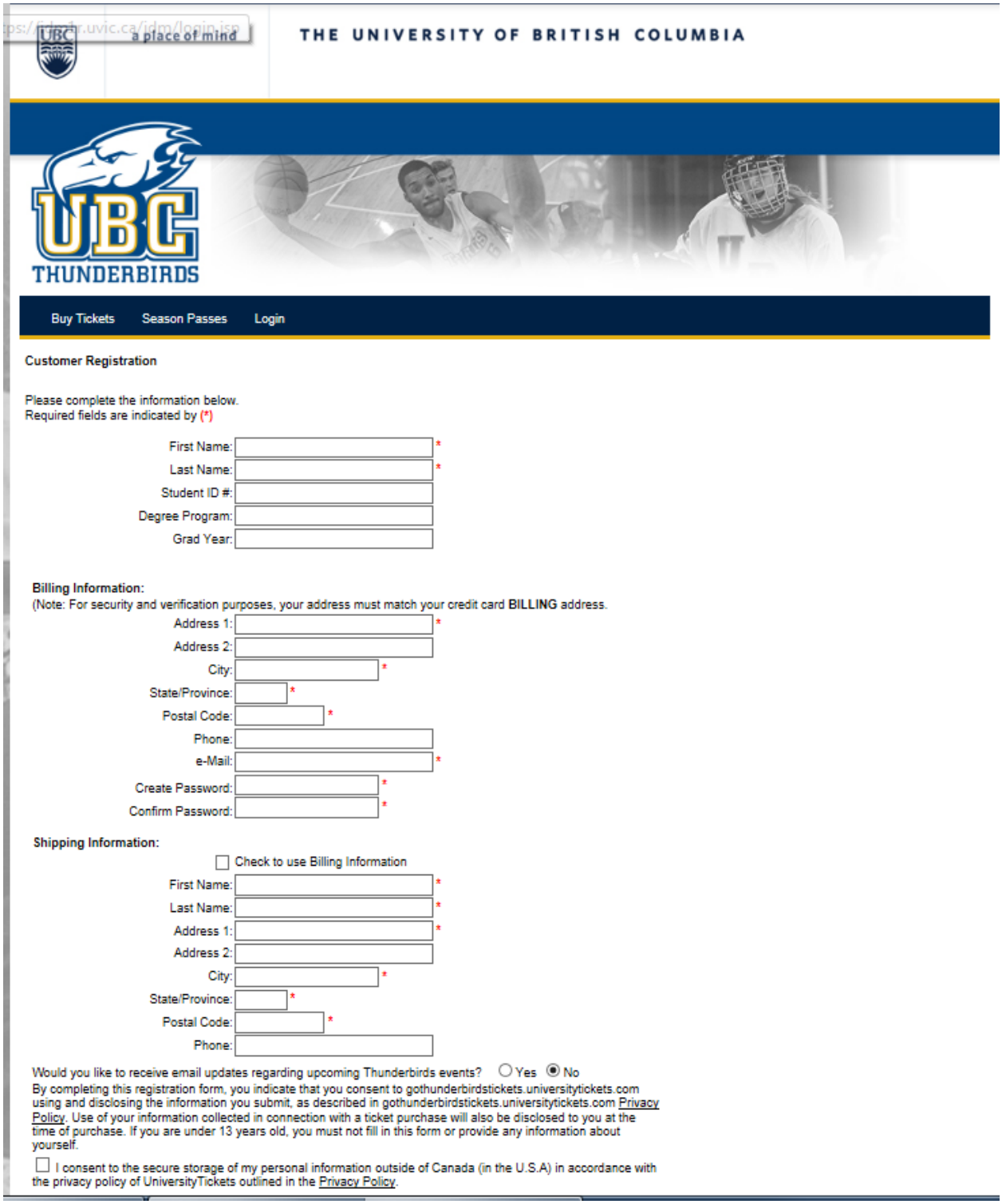
[[Enumerate all personally identifiable information (PII) data types stored in and accessed by the systems, and how these data types will flow in and out of the systems.]]

The personally identifiable information stored in the University Tickets system includes name, address, email address and phone number of community patrons who opt to purchase tickets online. It is collected directly from community patrons at the time of account creation and is used for payment validation at the time of purchase.

For community members purchasing tickets from the University Tickets solution, the form below (from UBC) shows the information gathered to create the client account:

http://gothunderbirdstickets.universitytickets.com/user_pages/customer_edit.asp?refpage=

(**note UVIC will not be collecting or showing fields for Student ID, Degree program or Grad year** – the non mandatory fields displayed in the UBC form).



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>1</td><td>Has a Privacy Impact Assessment ever been performed for this project or program?</td><td>[N]
[N/A]</td></tr>
<tr><td>2</td><td colspan="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

Vendor Privacy statement:
http://www.universitytickets.com/downloads/PrivacyPolicy.pdf</td></tr>
<tr><td>3</td><td colspan="2">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.

<table><tr><td>Highly Confidential</td><td>• [[Add a new bullet point for each data element]]</td></tr><tr><td>Confidential</td><td>• Name, Address, Email, Phone number, Payment information</td></tr><tr><td>Internal</td><td>•</td></tr><tr><td>Don't Know</td><td>•</td></tr></table></td></tr>
<tr><td>4</td><td>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?</td><td>[New]</td></tr>
<tr><td>5</td><td>Does the project apply new or additional information technologies that have substantial potential for privacy intrusion?

Cloud platform with US-based storage, mobile ticket scanning devices.
[[If so, what are those technologies?
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.)]]</td><td>[Y]</td></tr>
<tr><td>6</td><td>Will the project involve the collection or creation of new information about individuals?

[[If so, what information?]] Community patron PII and payment information will be collected by the vendor site.</td><td>[Y]</td></tr>
<tr><td>7</td><td>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?</td><td>[Y]</td></tr>
</table>

	[[If so, which organizations, processes or people?]] Community patrons will have PII stored in a US-based cloud vendor.	
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?]] PII is not currently collected from patrons of athletics events.	[Y]
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?]] Marketing information may be sent to community patrons on an opt-in basis.	[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+]	[5,001-50,000]
15	**Where will the information be stored?** Data stored in Amazon Eastern US data centres in Virginia.	
16	**Will a third party (e.g. vendor or service provider) have access to the information?** [[If so, which third parties?]] University Tickets and Amazon staff will have access to PII.	[Y]
17	**Is any of the information being accessed from outside of Canada?** [[If so, by whom and from where?]] All servers are located in an Sec. 15 facility in Sec. 15	[Y]
18	**Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems?** [[If so, which ones? This system will share PII with payment card providers. It is otherwise standalone and does not share data with any University systems. Examples include, but are not limited to: 1. Personal information is used in a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled). 2. Personal information is used in a system that has connections to at least one other system. 3. Personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	[Y]

	4. Personal information is transmitted using wireless technologies.]]	
19	**If there is external sharing, is it pursuant to new or existing information sharing agreements?** [[List these agreements]]	[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.
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.
4	Inappropriate or unauthorized use of PII by authorized individuals/processes/systems	1	1	Accept. All direct data access will be used in the completion of a transaction and / or online delivery of electronic tickets. Patrons who are concerned about inappropriate usage may acquire tickets in person at the ticket desk without providing any PII.
5	Unauthorized disclosure by individuals/processes/systems	1	1	Accept. All direct data access will be retained in the University Tickets system and will not be shared with other parties. Patrons who are concerned about inappropriate usage may acquire tickets in person at the ticket desk without providing any PII.
6	Creation of new PII by data matching	1	1	Mitigate. Potential for unauthorized matching mitigated by lack of integration with any UVic information systems.
7	Unauthorized tracking of individuals through transaction monitoring	1	2	Mitigate. Ensure clients opt in to any loyalty program. The system has the capability of tracking transaction history to reward high volume clients through a client loyalty program.
8	Data stored outside of Canada and in the public cloud	3	3	Mitigate. Disclose to clients that data is stored in a system outside of Canada.
9	Data retention beyond prescribed timeline	3	1	Mitigate. Project will investigate options for maintaining compliance with Directory of Records (DoR) data retention requirements.
10	Risk of increased surveillance	1	2	Same as 4 above.
11	Unauthorized use as a records repository	1	1	Accept. This solution is designated as a records repository for community patrons.
12	Public perception	1	1	Accept. The use of an electronic ticketing system would be expected by the general public and the campus community as it represents a modern and industry standard approach to ticketing.

13	**Use of existing PII data in a new system or business process**	1	1	**Accept. This information will be used for the stated purpose of completing an event ticket transaction and data collected is required to complete the transaction. Furthermore, there is no integration with other University 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	Y	Paul Stokes	Paul Stokes	TBD
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	Y	Garry Sagert	Tracey MacNeil	29-Oct-15
Production and Technical Support		Scott Thompson		
Development Services		Dave Wolowicz		
Identity Services		Corey Scholefield		
UVic Online		Garry Sagert		
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Infrastructure Services		Ron Kozsan		
Information Security Office		Eric van Wiltenburg		
Project Management Office	Y	Chandra Beaveridge	Chandra Beaveridge	TBD

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
Michelle Peterson		

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
Privacy Office	Bill Trott	Bill Trott	Phone call with Garry – Aug 2015 Oct 9, 2015, email and phone call with Tracey

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	21-Aug-15	Tracey MacNeil	Initial draft

0.2	25-Aug-15	Garry Sagert	Feedback / comments
0.3	24-Sept-15	Tracey MacNeil	Updates
0.4	27-Oct-15	Tracey MacNeil	Updates
0.5	27-Oct-15	Tracey MacNeil	Removed references to UVIC student and employee accounts created in the system. System will operate 'stand alone' for the launch.
0.6	16-Nov-15	Garry Sagert	Updates

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 PII maintained by University Tickets includes name, address, email address, phone number, payment information, and transaction history.

ID	PRIVACY CONTROLS
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**
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 All PII entered into University Tickets will be entered by the patron themselves at the time of account creation, following agreement to a notice of consent.
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 Patrons will have the ability to view and update their PII in University Tickets.

ID	PRIVACY CONTROLS
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 Patrons will have the ability to view and update their PII in University Tickets.
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. PII maintained by University Tickets includes name, address, email address, phone number, payment information, and transaction history.
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

ID	PRIVACY CONTROLS
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, The University Tickets system only shares data with payment card providers during purchasing transactions driven by community patrons. University Tickets is not integrated with any other information systems.

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 The University Tickets system only shares data with payment card providers during purchasing transactions driven by community patrons. University Tickets is not integrated with any other information systems.

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.]]

ID	SECURITY CONTROLS

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.]]

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 The University Tickets system only shares data with payment card providers during purchasing transactions driven by community patrons. University Tickets is not integrated with any other information systems.
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 does not contain nonpublic information;

ID	SECURITY CONTROLS
	• 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
	  • 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:** The University Tickets system only shares data with payment card providers during purchasing transactions driven by community patrons. University Tickets is not integrated with any other information systems.
CM-3	**Configuration Change Control**

ID	SECURITY CONTROLS
	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.]]

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:
	
	The components of the University Tickets solution include cloud-based online self-registration and ticket procurement software, and hand-held ticket scanners used by Athletics staff at event admission.

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:**

ID	SECURITY CONTROLS
	The organization develops a contingency plan for the information system. **Response:** Athletics will provide alternative methods of providing tickets in the event University Tickets is not available.
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). **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 All users are required to log in with their email address and a password they select upon account creation.
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:**

ID	SECURITY CONTROLS
	• 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.]]
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.]]

ID	SECURITY CONTROLS
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:** • 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.]]