University of Victoria

Sec. 15

Privacy Impact Assessment

Project Code	PC0492
Submission Date	April 2, 2015
Organization	University of Victoria
Unit	Purchasing Services
Contact	Annabelle Victoria, Purchasing Officer, Purchasing Services Chandra Beaveridge, Project Management Process Manager, University Systems
Reviewed By	Paul Stokes, Chief Information Officer, University Systems
Review Date	[[Date of review – can be filled in my PMO or Reviewer]]

ID	Risk Description	Likelihood (1-5)	Impact (1-5)
1	Lack of legal authority to collection, use or disclose PII	1	2
2	Unauthorized collection of PII by authorized individuals/processes/systems	1	2
3	Excessive collection of PII by authorized individuals/processes/systems	1	2
4	Inappropriate or unauthorized use of PII by authorized individuals/processes/systems	3	2
5	Unauthorized disclosure by individuals/processes/systems	1	2
6	Creation of new PII by data matching	1	1
7	Unauthorized tracking of individuals through transaction monitoring	1	2
8	Data stored outside of Canada and in the public cloud	5	2
9	Data retention beyond prescribed timeline	1	1
10	Risk of increased surveillance	3	3
11	Unauthorized use as a records repository	3	3
12	Public perception	2	4
13	Use of existing PII data in a new system or business process	1	1

Likelihood Scale
Impact Scale

1.0 Privacy Context

1.1 Description of Systems and Linkage to Legislation

Sec. 15 has been identified as a leading cloud-based purchasing tool to accept and evaluate electronic RFx submissions (RFP, RFQ, etc.) and has been piloted by Purchasing Services since December 2014. Electronic submission through Sec. 15 eliminates the requirement for hard copy submissions and allows Purchasing Services to keep all the RFx information electronically instead of paper filing. This electronic process also eliminates any timing concerns that the supplier may come across when trying to submit hard copies of bid documents. In addition, the software acts as the "time stamp" for the receipt of the submission which means that supplier can only submit proposals when the bidding process is open. Suppliers can no longer upload any documents once the RFx closes in Sec. 15 which eliminates the need for Purchasing Services to manually time stamp the receipts to prevent late submissions from being accepted.

Data submitted electronically through Sec. 15 is stored in a Canadian data centre. All data entered into Sec. 15 is transmitted through Sec. 15 a service with hosting that is distributed across various countries around the world [9].

This Privacy Impact Assessment (PIA) has been developed alongside the Project Plan to detail the risks and mitigation procedures associated with the use of this service at the University of Victoria.

1.2 Use of System

Sec. 15 will be used by selection committees comprised of UVic employees and graduate students, and Purchasing Officers for the purpose of managing public procurement document submissions (defined by Sec. 15 as a "project"), which includes the following activities:

- Creating and publically publishing procurement projects and RFx
- Accepting vendor documents and submissions
- Viewing, evaluating, and scoring submissions
- Scoring and evaluation criteria configuration
- Managing access to RFx evaluations and documents
- Communicating with selection committee members

Sec. 15 will be used by vendors who wish to bid on public procurement projects at the University of Victoria, which includes the following activities:

- Viewing publically published procurement projects at the University of Victoria
- Submitting RFx proposals and other documents for procurements

1.3 Custody and Control

All data disclosed or provided to Sec. 15 through the UVic Sec. 15 portal remains the right, title and interest of the University of Victoria [5].

Vendors who choose to submit information through Sec. 15 (section 1.4.4.2) provide Sec. 15 and Sec. 15 third party services with the right to use, copy, distribute, compress and process the data [11]. The Purchasing Officer must retrieve information submitted through Sec. 15 and the Sec. 15 email submission option (section 1.4.4.3). Data submission through these third party services is entirely optional for vendors and is provided as a fallback should the vendor be unable to submit documents via Sec. 15.

1.3.1 Collection

In compliance with FIPPA sections 21 and 26, the University of Victoria will collect personal information only as it relates to the administrative activities of the public procurement process. Any personal information submitted to Sec. 15

directly by the individual or vendor is considered to have been created with consent. In the case where personally identifiable information is submitted to Sec. 15 on behalf of another individual:

- Individuals must consent to the release of personal information as part of RFx documentation or research projects posted on their behalf by the Purchasing Officer solely for the purpose of conducting a public procurement.
- Purchasing Officers must only enter an individual's email address into Bonfire for the sole purpose of granting appropriate access to procurement documentation as part of selection committee membership.

1.3.2 Disclosure

Sec. 15 transmits all data submitted through the Sec. 15 Portal through a third-party service, Sec. 15 which has data centres outside of Canada. In compliance with FIPPA section 33.1, individual users must be informed and consent to the transmission of personally identifiable information outside of Canada. Sec. 15 notifies vendors that their data may cross outside of Canada. Purchasing Services will notify UVic employees and other selection committee participants of this risk through the confidentiality agreement that all committee participants must agree to as part of the procurement process.

Purchasing Officers can view the evaluations, ratings, and notes provided by each member of a project selection committee. This content may contain confidential information. All selection committee members will be notified by Purchasing Services in compliance with FIPPA section 26.

In compliance with FIPPA section 21, vendor submissions are not visible to other vendors. Vendor submissions are only visible to Purchasing Officers and selection committee members as designated by Purchasing Services.

1.4 Personally identifiable information Data Types and Information Flows

The Sec. 15 service collects personally identifiable information about selection committee participants and vendors who submit RFx Proposals. This information is stored and backed up in Canada, but Sec. 15 also transmits data through Sec. 15 to increase the stability of the service and to help protect the service against malicious attacks. Figure 1.0- Sec. 15 Data Flows shows the path that data submitted through the Sec. 15 web application takes before reaching Sec. 15 hosts in Montreal, QC and Kingston, ON.

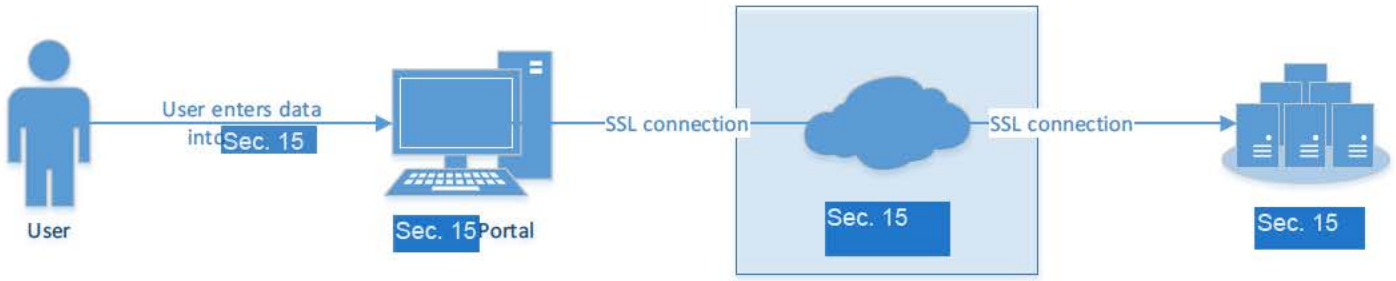


Figure 1.0 – Sec. 15 Data Flows

1.4.1 Sec. 15 Portal

The Sec. 15 Portal can be accessed through Sec. 15 The Portal has a public-facing site where potential vendors can view open projects and project details without logging into the service. All other Sec. 15 features and services, including the Sec. 15 ubmission Portal and selection criteria, can only be accessed after a user been granted appropriate permissions by a Purchasing Officer and received an email invitation to create an account by a Purchasing Officer.

Upon authentication, the Sec. 15 application creates a cookie that is encrypted before transmission to Sec. 15 (Fig 1.0). The Sec. 15 application does not support Single Sign-On (SSO) for authentication with UVic NetLink credentials. All

authentication credentials for Sec. 15 users are local to Sec. 15 and hashed and encrypted before storage. Credentials are not stored in plain text at any time.

Sec. 15

1.4.3 Sec. 15 Hosting and Backup

Sec. 15

1.4.4 Proposal Submission Solutions

Sec. 15 provides vendors with the ability to upload documents and submit on the uvic.bonfirehub.ca portal, as well as two backup options by which to upload and submit. It is recommended that vendors use the main Sec. 15 Submission Portal, but can also use the Sec. 15 dropbox service or email in their submission. Sec. 15 provides Sec. 15 Sec. 15 that vendors can use to request support directly from Sec. 15 support staff.

1.4.4.1 Sec. 15 Submission Portal

Sec. 15 has a Submission Portal for vendors to submit RFx proposals and supporting documents (Fig 2.0). Vendors must either log in to the portal with an existing user account or create a new one in order to submit documents for an RFx. All documents submitted through this process are hosted by Sec. 15 in Canada, but will be transmitted through Sec. 15 . The submission portal contains a link to the Terms of Service, which does specifically state that data may be hosted outside of Canada [6].

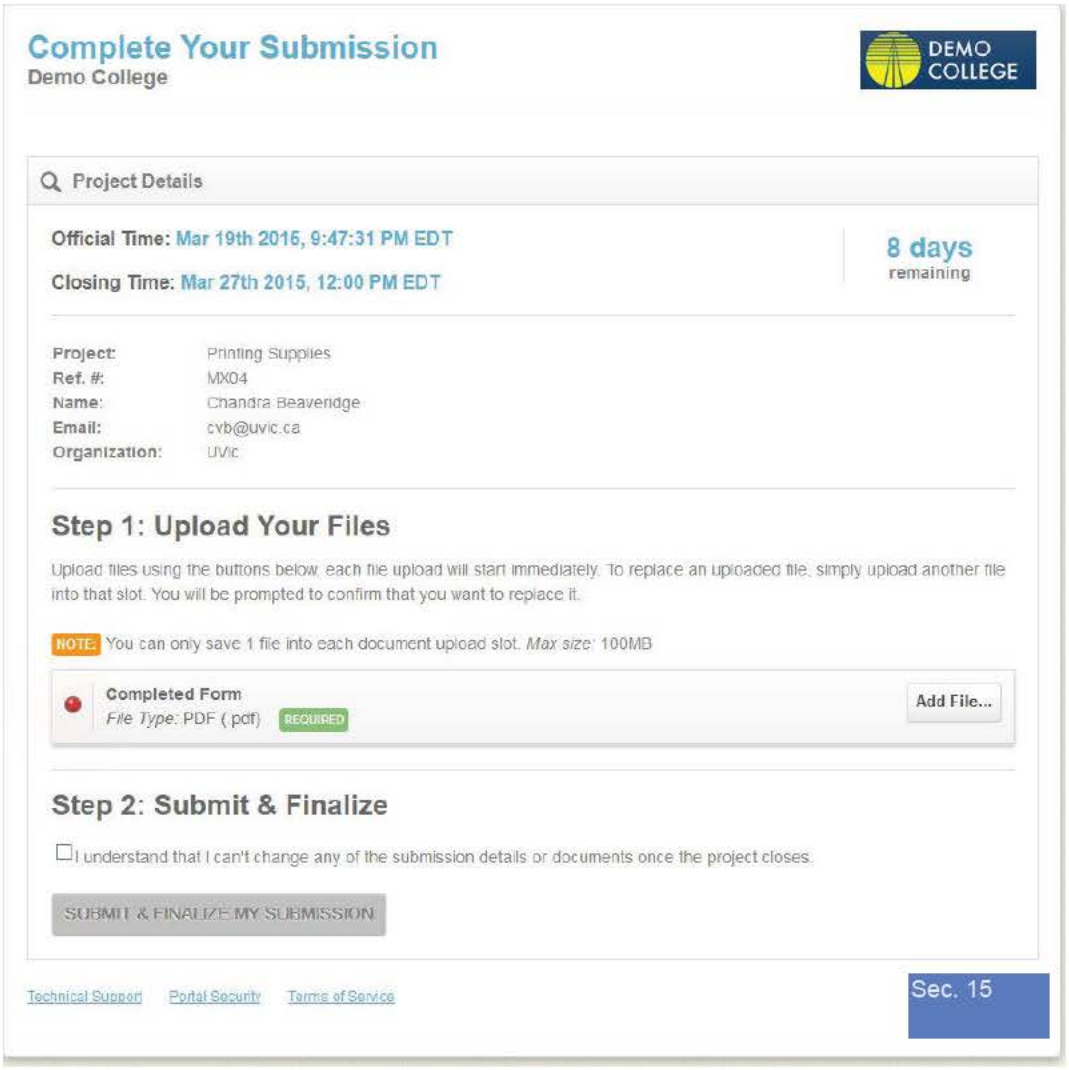
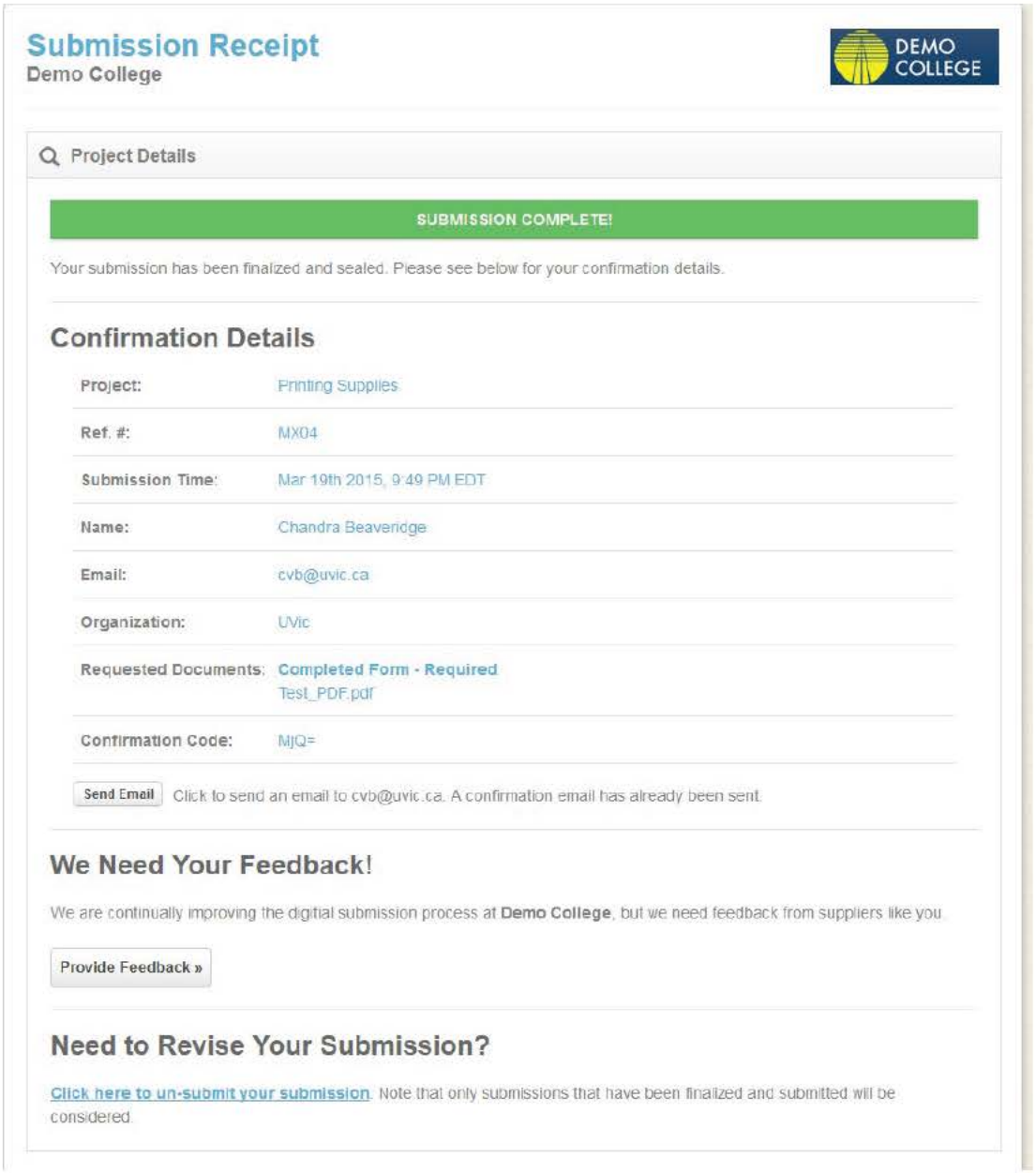


Figure 2.0-Sec. 15 Portal Vendor Upload

Vendors who choose to submit documents through the Sec. 15 Submission Portal will receive an on screen and email receipt to confirm the successful document submission (Fig. 3.0).



Submission Receipt

Demo College

DEMO COLLEGE

Project Details

SUBMISSION COMPLETE!

Your submission has been finalized and sealed. Please see below for your confirmation details.

Confirmation Details

Project:	Printing Supplies
Ref. #:	MX04
Submission Time:	Mar 19th 2015, 9:49 PM EDT
Name:	Chandra Beaveridge
Email:	cvb@uvic.ca
Organization:	UVic
Requested Documents:	Completed Form - Required Test_PDF.pdf
Confirmation Code:	MJQ=

Send Email Click to send an email to cvb@uvic.ca. A confirmation email has already been sent.

We Need Your Feedback!

We are continually improving the digital submission process at **Demo College**, but we need feedback from suppliers like you.

Provide Feedback »

Need to Revise Your Submission?

Click here to un-submit your submission. Note that only submissions that have been finalized and submitted will be considered.

Figure 3.0 Sec. 15 *Portal Vendor Upload Receipt*

The Sec. 15 Portal is also used by selection committee members to rate vendor proposals and submit notes to support the ratings.

Information Summary	
Usage	• Used by Purchasing Officers to post requests for proposals and other RFx types • Used by vendors to submit RFx responses • Used by Purchasing Officers to accept vendor responses within the response submission time limit • Used by Purchasing Officers to configure standard selection criteria rating schemes and processes • Used by Purchasing Officers and selection committees to view vendor responses and documents

	• Used by selection committees to document submission ratings and other notes
Source	• User created/submitted content
Data Fields	• Username and password • Email address • Vendor proposals and documentation • Public requests for proposals, bids, or other RFx • Selection criteria • Vendor proposal and documentation ratings • Selection committee notes
Classification	• Most selection committee participants and all Purchasing Officers are UVic employees and thus the contact information contained within Sec. 15 about these individuals is not considered of confidential nature in accordance with FIPPA. • Some selection committee participants may be students. Contact information is considered personal information in accordance with FIPPA. • Vendor submissions may contain personally identifiable information, trade secrets, commercial, financial, scientific, or technical information in accordance with FIPPA. • Selection criteria and selection committee notes may contain confidential business information about vendors and/or confidential research information as it pertains to project(s) related to the procurement.
Authority	FIPPA Sections 21, 22.4 (f), 33.1
Information Flow	• All information is manually entered by the Purchasing Officer, vendor, or selection committee. Information is then transmitted through Sec. 15 (1.4.2) before arriving back in Canada for storage and backup.
Access	• Full administrative access is restricted to Purchasing Officers only • Purchasing Officers assign appropriate selection committee permissions • Vendors do not have access to the data submitted by other vendors
Risks	• Exposure of personally identifiable and business information outside of Canada

1.4.4.2 Sec. 15

Sec. 15 is a third party file sharing platform that Sec. 15 offers to vendors who are unable to use the Submission Portal or email to provide RFx submissions (Fig. 4.0). A vendor can access this service from th Sec. 15 page within Sec. 15 and must agree to the Sec. 15 provided by Sec. 15 o use this submission method. The Sec. 15 Sec. 15 states:

If you are located outside the United States, you should be aware that Sec. 15 ransfers Personal Information and Non-Identifying Information to the United States and processes it there. Your use of our Services represents your agreement to such transfer. [12]

Sec. 15

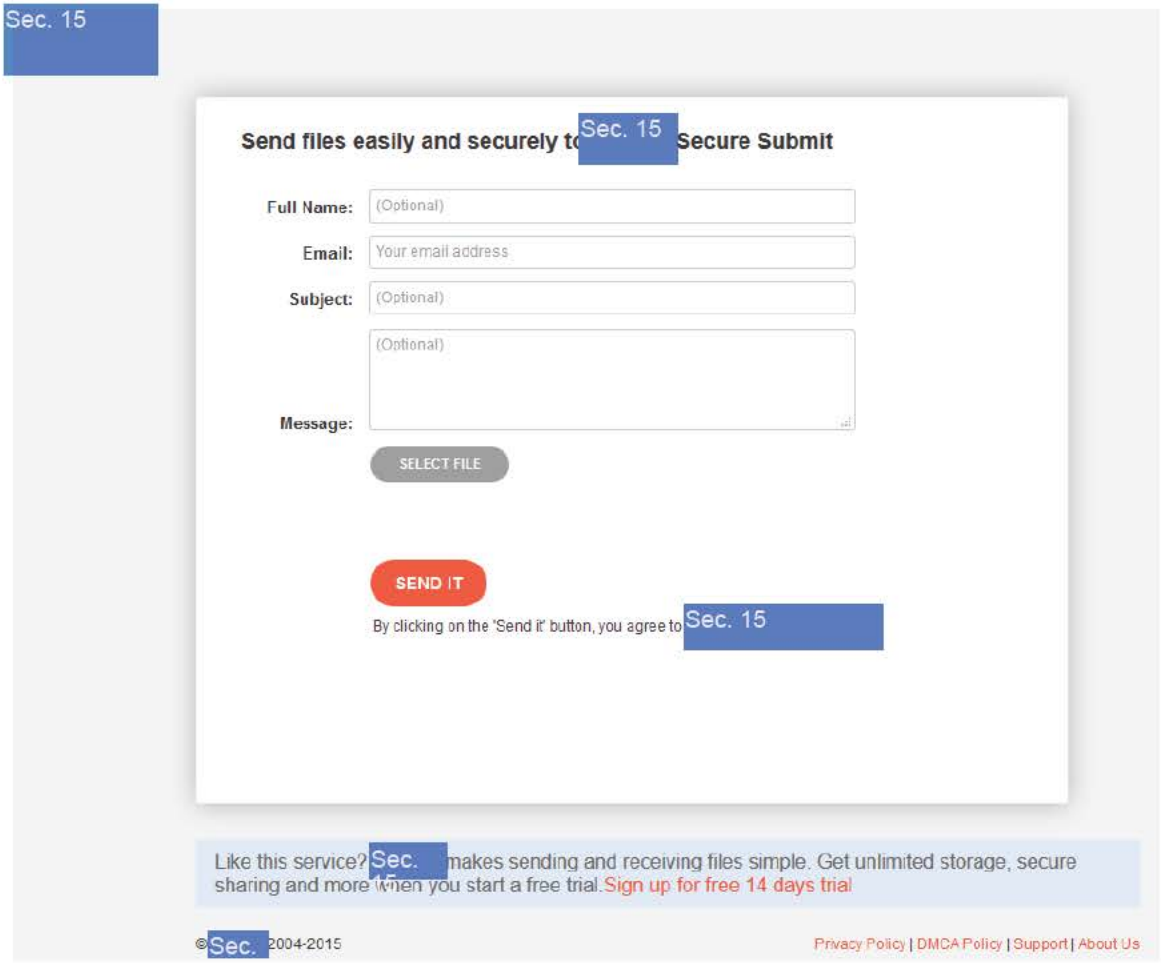


Figure 4.0- Sec. 15 Dropbox Vendor Uploader

Vendors who choose to submit documents through Sec. 15 will receive an on screen and email receipt to confirm the successful document submission (Fig 5.0).

Sec. 15

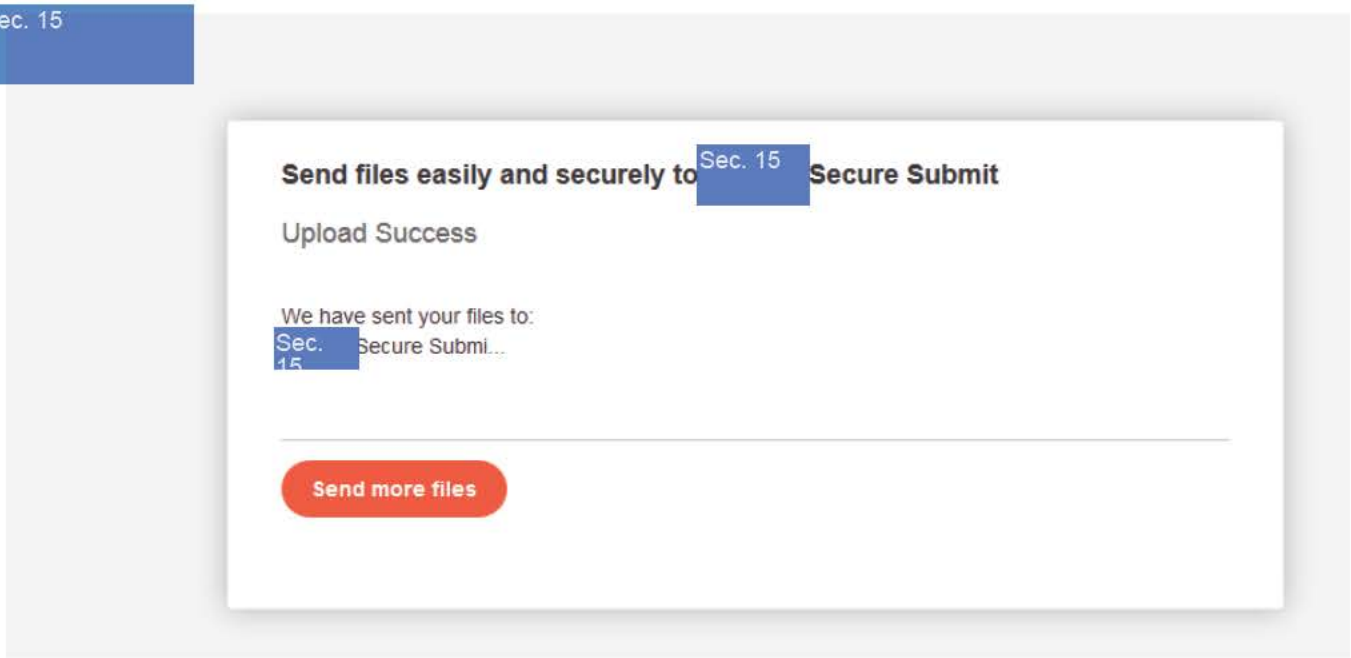


Figure 5.0- Sec. 15 Vendor Upload Receipt

Information Summary	
Usage	• Used by vendors to submit RFx responses • Used by Purchasing Officers to accept vendor responses within the response submission time limit
Source	• User created/submitted content
Data Fields	• Email address • Vendor proposals and documentation
Classification	• Vendor submissions may contain personally identifiable information, trade secrets, commercial, financial, scientific, or technical information in accordance with FIPPA.
Authority	FIPPA Sections 21, 22.4 (f), 33.1
Information Flow	• All information is manually entered by the vendor. The submission is then available to Purchasing Services through Sec. 15 for inclusion in the RFx project.
Access **Risks**	• Vendors can submit documents using an online form. • Purchasing Officers retrieve documents through Sec. 15 • Exposure of personally identifiable and business information outside of Canada

1.4.4.3 Email

Vendors can email RFx submissions as attachments to Sec. 15 if they are unable to use the Submission Portal. Email submissions to Sec. 15 are received by Sec. 15 support staff.

Information Summary	
Usage	• Used by vendors to submit RFx responses • Used by Purchasing Officers to accept vendor responses within the response submission time limit
Source	• User created/submitted content
Data Fields	• Email address • Vendor proposals and documentation
Classification	• Vendor submissions may contain personally identifiable information, trade secrets, commercial, financial, scientific, or technical information in accordance with FIPPA.
Authority	FIPPA Sections 21, 22.4 (f), 33.1
Information Flow	• All information is manually emailed by the vendor. The submission is then provided to Purchasing Services by Sec. 15 support through email for inclusion in the RFx project.
Access **Risks**	• Vendors can submit documents via email. • Purchasing Officers retrieve documents through Sec. 15 upport. • Exposure of personally identifiable and business information outside of Canada.

2.0 Privacy Threshold Analysis

This Privacy Threshold Analysis was completed with and reviewed by the Project Sponsor.

1	Has a Privacy Impact Assessment ever been performed for this project or program?	No
2	Does the project collect, maintain, or share personally identifiable information (PII) in any identifiable form?	Yes
3	What is the information classification level[1] of the information? (multi-select) • Highly Confidential • Confidential • Internal • Public	Public (P) Internal (I) Confidential (C) Highly Confidential (HC)
4	What are the type(s) of information? (multi-select) *Examples include, but are not limited to information about students, employees, donors, alumni, credit cards, health Information, etc.*	- Product and service information (P) - Employee directory listing content (P) - Budget information (I) - Select Unit procedures (I) - Information protected by non-disclosure agreements (C) - Contract information (C) - Certificate/license numbers, device IDs and serial numbers, email, URLs, IP addresses (C) - Confidential information in Contracts (C) - User account passwords (C) - Authentication credentials (HC)
5	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 information?	This new system supports the creation, collection, storage, back-up, and disposition of the information listed above.
6	Does the project apply new or additional information technologies that have substantial potential for privacy intrusion? *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.)*	Yes, Sec. 15 is a Software as a Service cloud platform.
7	Will the project involve the collection or creation of new information about individuals?	Yes, information about vendors who submit RFx proposals will be collected through Sec. 15

[1] Levels are Public, Internal, Confidential, Highly Confidential; see IM7800, Information Security Classification Procedures, for detailed definitions.

8	Will personal information about individuals be disclosed to organizations, programs, processes or people who have not previously had routine access to the information?	No
9	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	No
10	Will the project collect, use, or disclose PII for research purposes?	No
11	Will the project require that individuals are contacted in ways that they may perceive to be intrusive?	No
12	Is any of the information owned by another organization?	Yes
13	Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	No
14	Does this project collect, access or use Social Insurance Numbers (SIN)?	No
15	How many user records containing PII will be stored, accessed or used? [1-1000],[1001-5000],[5,001-50,000],[50,001-100,000],[100,000+]	Sec. 15
16	Where will the information be stored? *Examples include, but are not limited to the UVic Data Centre, providers within Canada, providers outside of Canada.*	Sec. 15 is hosted in a Canadian data centre in Montreal QC. The failover data centre is located in Kingston ON. All data entered into Sec. 15 is transmitted through Sec. 15 which is hosted in the United States. Access log files containing Sec. 15 data could be stored for several hours on servers hosted outside of Canada. Access logs contain: IP Address Resource being requested Requested type Request time Vendors may choose to submit data through Sec. 15 or via email. Both services host data outside of Canada.
17	Will a third party (e.g. vendor or service provider) have access to the information?	Yes, the Sec. 15 support team will have access to unencrypted data that has been entered into Sec. 15
18	Is any of the information being accessed from outside of Canada?	All data entered into Sec. 15 is transmitted through Sec. 15 which is hosted world-wide.

		Vendors may choose to submit data through Sec. 15 or via email. Both services transfer data outside of Canada.
19	Does the IT system connect, receive, or share information in identifiable form or PII with any other IT systems? 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. 4. Personal information is transmitted using wireless technologies.	Sec. 15
20	If there is external sharing, is it pursuant to new or existing information sharing agreements?	No

3.0 Privacy & Security Risks

The likelihood and impact of risks defined below have been determined using the Likelihood Scale and Impact Scale referenced on the University of Victoria Financial Planning and Operations website.

Risk 1 - Lack of legal authority to collection, use or disclose PII

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 2
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 2 - Unauthorized collection of PII by authorized individuals/processes/systems

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 2
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 3 - Excessive collection of PII by authorized individuals/processes/systems

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 2
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 4 - Inappropriate or unauthorized use of PII by authorized individuals/processes/systems

Risk Profile	
Risk Score	Likelihood: 3
	Impact: 2
Privacy Controls	DM-1, SE-2
Security Controls	AC-2, AC-3, AC-4, AC-8, AC-21, AT-2, AU-6
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent. Mitigate: Purchasing Officers will grant and revoke access to procurement projects in Sec. 15 as appropriate
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 5 - Unauthorized disclosure by individuals/processes/systems

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 2
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent. Mitigate: Purchasing Officers are the only users who can post information publically.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 6 - Creation of new PII by data matching

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 1
Risk Response	Mitigate: Sec. 15 does not interconnect or data match with other systems. All data is input manually for individual projects.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 1

Risk 7 - Unauthorized tracking of individuals through transaction monitoring

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 2
Risk Response	Sec. 15
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 8 - Data stored outside of Canada and in the public cloud

Risk Profile	
Risk Score	Likelihood: 5
	Impact: 2
Privacy Controls	DM-1, SE-2
Security Controls	AC-2, AC-4, AC-8, AC-19, AC-20, AC-21, AC-22, AT-2, AU-6, CM-10, CP-9, IA-2, IA-8, MP-2, PE-3, SC-7, SC-8, SI-12
Description	All data submitted through Sec. 15 is transmitted out of Canada through Sec. 15 Vendor submissions to Hightail or through the Sec. 15 email submission service are also transmitted outside of Canada.
Risk Response	Sec. 15

	Sec. 15
Residual Risk after Mitigation	Likelihood: 5
	Impact: 1

Risk 9 - Data retention beyond prescribed timeline

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 1
Security Controls	SI-12
Risk Response	Mitigate: Purchasing Services can contact Sec. 15 at any time to have data permanently destroyed. Sec. 15 can also set up regular deletion of data on a prescribed schedule.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 1

Risk 10 - Risk of increased surveillance

Risk Profile	
Risk Score	Likelihood: 3
	Impact: 3
Privacy Controls	AP-2, DM-1, IP-1
Security Controls	AC-3
Description	Purchasing Officers have the ability to view individual actions within Sec. 15 such as evaluation progress of an individual selection committee member.
Risk Response	Mitigate: The Purchasing Officer must inform selection committee users that their evaluation progress and actions within Sec. 15 can be viewed before user account creation.
Residual Risk after Mitigation	Likelihood: 2
	Impact: 2

Risk 11 - Unauthorized use as a records repository

Risk Profile	
Risk Score	Likelihood: 3
	Impact: 3
Security Controls	SI-12
Description	Sec. 15 could be used as an official records repository for RFx evaluations and/or vendor submissions as it provides the storage and organizational functionality to do so.
Risk Response	Mitigate: Purchasing Services will continue to keep official local copies of evaluations and submissions outside of Sec. 15 using existing processes in compliance with FIPPA section 30.1. Records in Sec. 15 will be considered transitory and not official. Records within Sec. 15 will be purged as per SI-12.
Residual Risk after Mitigation	Likelihood: 1
	Impact: 2

Risk 12 - Public perception

Risk Profile	
Risk Score	Likelihood: 2
	Impact: 4
Privacy Controls	DM-1, SE-2

Security Controls	AC-2, AC-4, AC-8, AC-19, AC-20, AC-21, AC-22, AT-22, AU-6, CA-3, CM-10, CP-9, IA-2, IA-8, MP-2, PE-3, SC-7, SC-8, SI-12
Description	Although the Sec. 15 service is hosted in Canada, data submitted to Sec. 15 is transmitted outside of Canada. This could raise privacy concerns from vendors and selection committee users who wish to participate in a procurement project.
Risk Response	Mitigate: In accordance with the response in DM-1, all efforts will be made to reduce the amount of Personally Identifiable Information required for selection committee members to participate. In the event that a selection committee member is uncomfortable using the service, Purchasing Services will work with the project team to determine if a replacement selection committee member can be found. Mitigate: In the event that a vendor is uncomfortable using the service, the vendor can contact the Director of Purchasing Services to evaluate alternate methods by which to submit their proposal.
Residual Risk after mitigation	Likelihood: 1
	Impact: 3

Risk 13 - Use of existing PII data in a new system or business process

Risk Profile	
Risk Score	Likelihood: 1
	Impact: 1
Description	All PII will be entered by the individual or on behalf of the individual with consent. There will be no existing PII from other systems imported into Sec. 15
Risk Response	Mitigate: PII entered into Sec. 15 is submitted directly by the user or on behalf of the user with consent.
Residual Risk after mitigation	Likelihood: 1
	Impact: 1

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		May 7, 2015
Systems General Office		Trish Kearley		
Client Technologies		Lance Grant		
Desktop Support Services		David Street		
Computer Help Desk		Marcus Greenshields		
Academic & Admin Services	Y	Nav Bassi		April 8, 2015
Client Account Managers	Y	Garry Sagert		April 17, 2015
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		May 7, 2015

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 system owner.

Name	Comments	Date of Consultation
Annabelle Victoria		April 29, 2015

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
Sec. 15			May 14, 2015

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	February 6, 2015	Chandra Beaveridge	Used PTA answers to begin document
1.1	February 28, 2015	Chandra Beaveridge	Incorporated responses received from Sec. 15 into the PIA

1.2	March 13, 2015	Chandra Beaveridge	Quick notes from conversation with Garry and Alex
1.3	March 19, 2015	Chandra Beaveridge	Refined notes from March 13 meeting, added charts for data flows
1.4	March 20, 2015	Chandra Beaveridge	Filled out most of the controls
1.5	March 24, 2015	Chandra Beaveridge	Worked on controls
1.6	April 1, 2015	Chandra Beaveridge	Finished custody & control and risks
1.7	April 2, 2015	Chandra Beaveridge	Added additional screen shots, links to supporting vendor documentation
1.8	April 21, 2015	Chandra Beaveridge	Incorporated feedback from Paul, Nav, and Garry
1.9	May 4, 2015	Chandra Beaveridge	Incorporated changes from Purchasing
2.0	May 7, 2015	Chandra Beaveridge	Verified sources, fixed formatting of risks section
2.1	May 7, 2015	Chandra Beaveridge	Incorporated final feedback from Paul
2.2	May 14, 2015	Chandra Beaveridge	Incorporated feedback from Alex
2.3	June 2, 2015	Chandra Beaveridge	Adjusted question 4 in the PTA.

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 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.

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.
	
	Purchasing Officers are responsible for granting and revoking access to procurement projects within Sec. at project commencement and closure. Selection committee users will receive email notifications from Sec. as their access to projects is added or removed.
	
	The Director of Purchasing Services will authorize the addition or removal of Purchasing Officer administrator access to Sec.

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 Anyone can sign up for vendor access to Sec. to submit RFx proposals and documents. Vendor access is limited to viewing public procurement request information from the University of Victoria and the submission of data. Vendors cannot view other vendor submissions.

ID	SECURITY CONTROLS
	Purchasing Officers are responsible for granting access to particular procurement projects and inviting selection committee members to sign-up for an account via email. Purchasing Officers can assign and revoke access to Sec. entirely, or to particular projects as appropriate. By default, Purchasing Officers can view all scores on a particular project. Selection committee members cannot see each other's scores unless the Purchasing Officer specifically enables this option. A user's permissions are checked by Sec. upon each view or action change. Access will be denied to users who attempt to access a view or feature that is not permitted. Sec. is configured to expire and destroy user sessions if suspicious activity is detected, which includes attempting to access a part of the application that is not available to a given user [1].
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 Only active staff or students will have access to Sec. as selection committee members. Access will be provided and revoked by Purchasing Services. Any vendor can submit responses for RFx in compliance with th Sec. 15 Terms and Conditions, FIPPA, and University Policies. Content will be securely transmitted over HTTPS, see Fig 1.0.

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:
	
	Sec. does not display an organization-defined system use notification message or banner before granting access to the system. A Terms of Service is listed in the Sec. Portal at all times and a Terms of Service is also available for those who wish to use the Sec. document upload service. These terms have been created by their respective organizations and pertain only to vendor interaction with Sec.
	
	The Purchasing Officer responsible for granting access to Sec. 15 will send an email to every selection committee participant containing the following information upon initial invitation to the service:
	
	• 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

ID	SECURITY CONTROLS
	• 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

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
	
	Sec. 15 does not recommend that clients use Sec. 15 from mobile devices. This is not the supported method of accessing this service [7].

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
	
	Use of the Sec. Service is enforced under the following Sec. agreements:
	Sec. 15
	Sec. Policies within the Sec. 15 [1] document:
	POLICY: Data Centre Supplier Requirements
	POLICY: Support & Incident Management
	POLICY: Employee Data Access
	POLICY: Data Destruction Policy
	
	Use of the OVH Service is enforced under the following OVH agreements:
	Sec. 15 [14]
	
	Use of the Sec. 15 Service is enforced under the following Sec. 15 agreements:
	Sec. 15
	
	Use of Sec. 15 is enforced under the following Sec. 15 agreements:
	Sec. 15
	
	Use of Sec. is enforced under the following Sec. agreements:
	Sec. 15

ID	SECURITY CONTROLS
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 Purchasing Officers are responsible for assigning user roles and authorization to share content on Sec. 15 Purchasing Officers and selection committee members (if permitted by the Purchasing Officer) can post project documentation to the public on Sec. 15 Purchasing Officers and selection committee members can share selection criteria, notes, and scores internally within the Sec. system using memberships defined by the Purchasing Officer. Sec. verifies user permissions on every page view and action to determine if a user should be able to view or act upon certain content. If a user attempts to deep link to a page that they do not have access to, Sec. will redirect the user to the main public portal page [1].
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; • 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 Purchasing Officers are responsible for designating who is authorized to post publically accessible information in Sec. and are respons ble for reviewing content before it is posted publically.

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:

ID	SECURITY CONTROLS
	Purchasing Officers are responsible for notifying selection committee members that information entered into Sec. is transmitted outside of Canada. All selected members must consent before being a part of the selection committee and joining Sec. 15 Vendors are notified that information submitted to Sec. is transmitted outside of Canada through the Sec. 15 Sec. 15 Vendors who choose to use Sec. for document submission will be notified that data is transmitted and stored outside of Canada through the Sec. Sec. 15 and Sec. Sec. Vendors will not be prompted to read any of these documents before creating an account and submitting documents, but these agreements are posted on the document submission pages.
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:** Cookies are used to store user session information for users that are logged in to Sec. Sec. logs user activities and will destroy user sessions if suspicious activity is registered (e.g. attempting to access parts of the portal that a user does not have permission to access or a sudden change in a user's IP address.) [1] Sec. will check a user's permissions on page view or action to ensure that the user should have access to the information [1]. Sec. monitors the application, infrastructure load, and performance. If the application produces server or client-side errors (e.g. JavaScript errors), the Sec. technical team is notified by email [1]. All data centre staff access to Sec. servers is logged. Servers are monitored by on-site technicians 24 hours a day, 7 days a week [1]. See POLICY: Support & Incident Management D. PRIVACY AND SECURITY for privacy and security breach responses [1]. Sec. 15 keeps logs of Sec. site visitors for approximately 4 hours. Further information is available at Sec. 15 15 7]. If Purchasing Services is contacted by Sec. regarding a privacy or security breach, Purchasing will contact the Chief Privacy Officer or Information Officer. Limited reporting records are available by self-service to Purchasing Officers within the application. This includes changes in scores and last authentication by a particular user. Executive summary and scoring reports can be generated within the application and downloaded by the Purchasing Officer for record keeping and offline use. [8] Apache access logs are available to Sec. staff and can be reviewed by the University of Victoria upon request for further diagnosis and troubleshooting. This information is not available within the Sec. application. [8]
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].

ID	SECURITY CONTROLS
	Response: Sec. is not interconnected to other information systems at the University of Victoria. Any and all Sec. data is manually entered or uploaded by Purchasing Officers, selection committee members, or vendors. In the event that a Purchasing Officer cannot enter or upload information into Sec. , a Purchasing Officer could contac Sec. technical support and authorize their assistance to upload data into Sec. Sec. 15 Sec. is not directly connected to Sec. 15 is a separate service that vendors can use to submit documents if they are unable to use the upload feature in Sec.
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 by Sec. 15 • Sec. 15 will notify Purchasing Services by email of any configuration changes, updates/patches, and planned or unplanned outages. The University of Victoria are not responsible for testing any patches or releases. When Sec. does notify Purchasing Services of a new feature, Purchasing Services must contact Sec. to have this feature enabled [7].

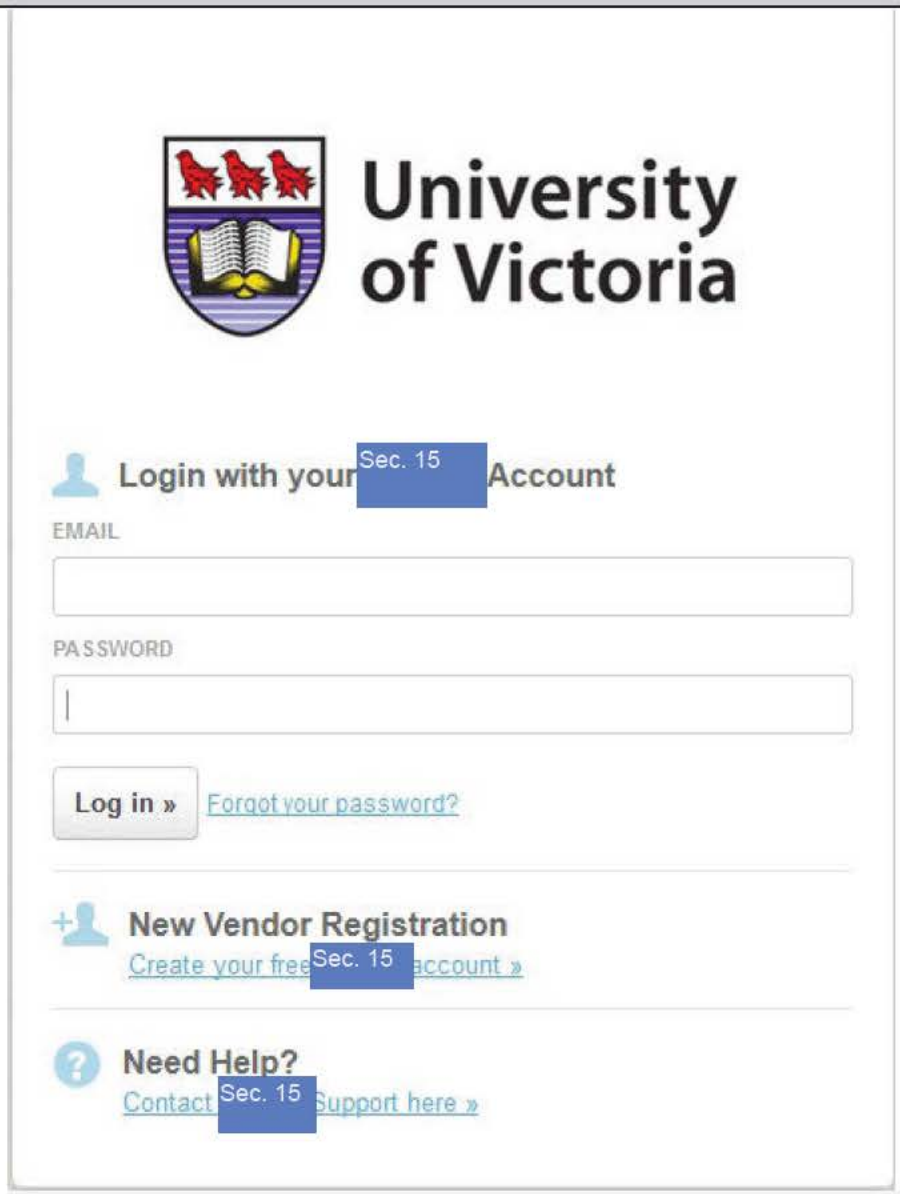
CM-8	**Information System Component Inventory**
	
	Control:
	
	• Develops and documents an inventory of information system components that:
	  • Accurately reflects the current information system;
	  • Includes all components within the authorization boundary of the information system;
	  • Is at the 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:
	
	Sec. 15
	Sec. 15 Application servers and database
	Sec. 15 – Application and database backup
	Sec. 15 SSL, DNS, and malicious attack protection services

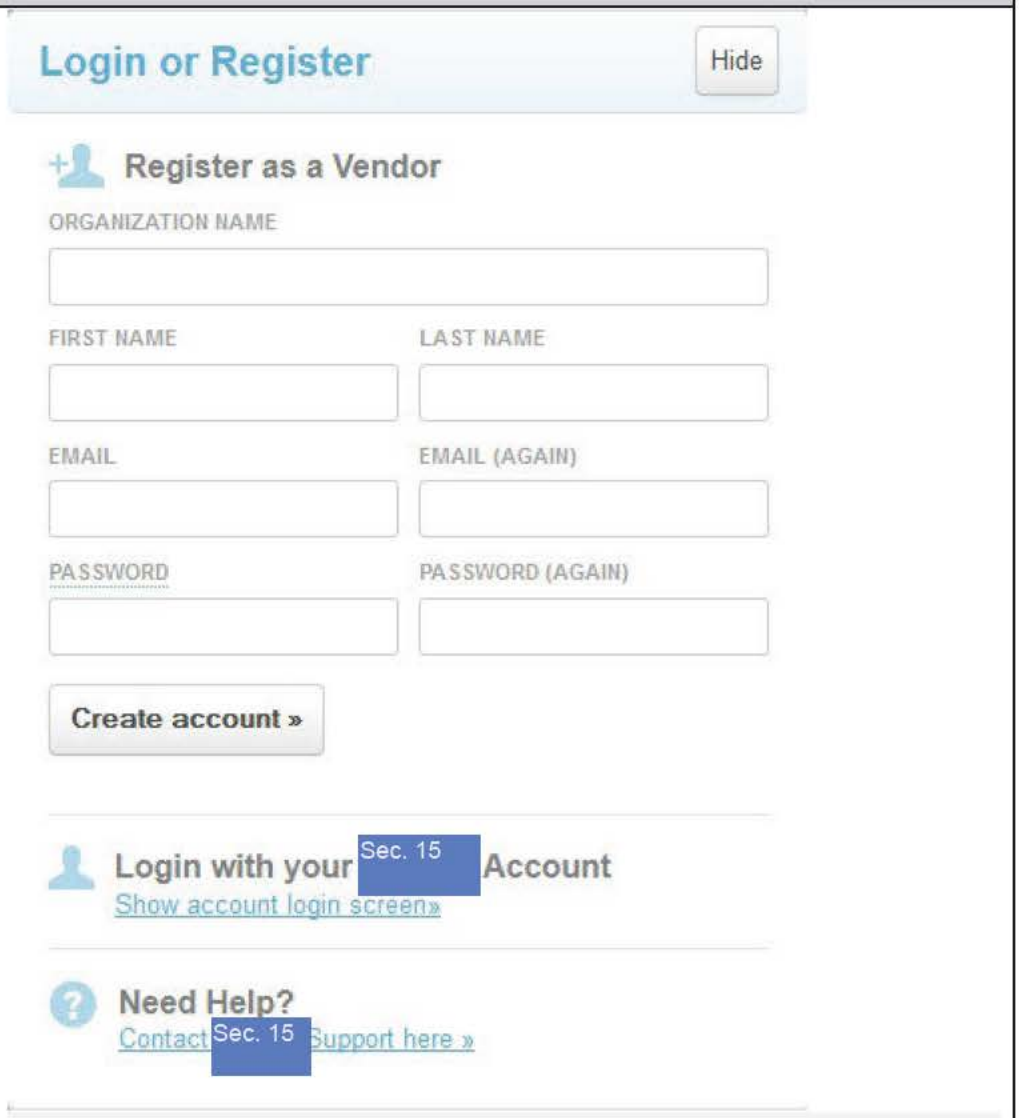
ID	SECURITY CONTROLS
	Sec. 15 and email be used by the vendor to submit documents, but neither are directly connected to

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:
	
	• Use of Sec. 15 is governed by the following policies and legislation:
	  • 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
	  • Freedom of Information and Protection of Privacy Act (FIPPA) http://www.bclaws.ca/Recon/document/ID/freeside/96165_00
	System use to post projects, develop selection criteria, and view and rate vendor submissions is limited to Purchasing Officers and those authorized by Purchasing Officers.
	
	See AC-20

CP-2	**Contingency Plan** **Control:** The organization develops a contingency plan for the information system. **Response:** Sec. 15 provides a 99.9% up-time guarantee. The Sec. 15 and email submission methods can be used by the vendor at the risk of the vendor should the vendor not be able to submit documentation through Sec. 15 Sec. 15 is not considered an official records repository. In the event that Sec. 15 is unavailable, Purchasing Services will accept vendor proposals as per existing processes. All data stored within Sec. 15 can be exported to the University of Victoria in the event that the portal is not recoverable. See **SI-12.** See F. Disaster Recovery and System Recovery in the Sec. 15 Overview document.
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

ID	SECURITY CONTROLS
	documentation including security-related documentation; and Protects the confidentiality, integrity, and availability of backup information at storage locations. **Response:** Sec. 15
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 If a selection committee member should have access to Sec. , a Purchasing Officer will associate the correct permission set with the email address of the user and send the user an invitation through the Sec. portal. The user will receive an email with a link to create a unique username and password to access the service. The user will have the assigned permissions upon login. Sec. 15 Sec. 15

ID	SECURITY CONTROLS
	
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 Any member of the public can create an account through Sec. 15 to submit responses to RFx. Sec. 15 Sec. 15

ID	SECURITY CONTROLS
	
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:** Purchasing Officers define the level of access that selection committee members should have access to. Access can be defined per project (including project documentation) to prevent users from having access to additional procurement data. Purchasing Officers can also revoke access to projects. Sec. 15 permissions are checked upon each page load and user action to ensure that only authorized users access digital media submitted by vendors. Vendor access is limited only to the submission of media and public viewing of RFx posted by Purchasing Officers.
PE-3	**Physical Access Control** **Control:**

ID	SECURITY CONTROLS
	• Enforces physical access authorizations, controls and audits exist. **Response:** Sec. 15
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 See POLICY: Employee Data Access Sec. 15 Security Overview) [1]
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.
SC-7	**Boundary Protection** **Control:**

ID	SECURITY CONTROLS
	• 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:** Sec. 15
SC-8	**Transmission Confidentially and Integrity** **Control:** • The information system protects the confidentiality and; integrity of transmitted information. **Response:** Sec. 15
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:** Sec. 15 automatically notifies a user by email when the user: - Is invited to create a Sec. 15 account (Purchasing Officer prompted action) - Wishes to reset his or her password (user prompted action) - Is provided with access to a project (Purchasing Officer prompted action) - Has his or her access to a project revoked (Purchasing Officer prompted action) - Submits a proposal for a project (user prompted action) - Is reminded that an evaluation is incomplete or a deadline is approaching (Purchasing Officer prompted action) Emails are sent to users from notifications@Sec. 15 Sec. 15 automatically notifies a user by email when the user: - Submits a proposal for a project (user prompted action) - Sec. 15 will blacklist email addresses that are repeatedly used in suspicious submissions [13] Emails are sent to users from delivery@Sec. 15
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 - After a retention period that the University of Victoria will specify on the Order Form, Purchasing Services will be contacted regarding the destruction of data stored with Sec. . At this time, Purchasing Services will be given the option to perform a data export. Records will not be destroyed if there is an active investigation or court case involving data stored in Sec. 15 - When a project is deleted in Sec. a record of that project is kept in order to maintain compliance for FIPPA or other legal requests. These records are destroyed when a request is escalated as per the data retention period as define on the Order Form [1]. - If the University of Victoria and Purchasing Services chooses to cancel the Sec. service or chooses not to renew the contract after 3 years, the option to export the data will be presented and the data will be permanently destroyed upon request. Records will not be destroyed if there is an active investigation or court case involving data stored in Sec. [7].

Appendix C – References

The following documents were used in the creation of this PIA.

[1] Sec. 15

[2]

[3]

[4] Sec. 15

[5]

[6] last accessed May 7, 2015

[7] Information obtained verbally with Sec. 15, on March 13 and May 7

[8] Information obtained through email with Sec. 15 February-May, 2015

[9] Sec. 15 last accessed May 7, 2015

[10] Sec. 15 last accessed May 7, 2015

[11] Sec. 15 last accessed May 7, 2015

[12] Sec. 15 last accessed May 7, 2015

[13] Information obtained verbally with Sec. 15 technical support, May 7, 2015

[14] Sec. 15 last accessed May 7, 2015

[15] Sec. 15 15 last accessed May 7, 2015

[16] last accessed May 7, 2015