# ATRS InnoSoft Fusion Privacy Impact Assessment

| | |
|---|---|
| Project Code | PC0745 |
| Submission Date | July 24, 2017 |
| Organization | University of Victoria |
| Unit and Service Owner | Vikes Athletics and Recreation |
| Contact | Jan Misovic, Senior Desktop Support Analyst, University Systems |
| Reviewed By | [[The CIO or designate responsible for reviewing this PIA.<br>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

The University of Victoria's Vikes Athletics and Recreation (ATRS) provides services to varsity athletes, students, faculty and staff as well as users from the local community. These services include varsity sports programs, membership sales, instructional and fitness programs, intramural leagues, aquatics, a fitness and weights center, a climbing wall, sports clubs, summer camps, facility rentals, drop-in activities, point of sale (POS), and equipment lending.

Vikes Athletics and Recreation has used ACTIVE Network's CLASS recreation management software since 2007. The CLASS system has played a crucial role in the management of the department's daily business operations. CLASS is scheduled to reach end-of-life after November 2017.

Project PC0651 (ATRS Recreation Management System RFP) was completed to identify a suitable enterprise-level replacement. Based upon the proposals received and a comprehensive selection process, InnoSoft Fusion (http://www.innosoftfusion.com) was identified as the preferred solution for Vikes Athletics and Recreation. InnoSoft offers self-hosted and fully hosted options. Fusion offers an all-in-one solution to campus recreation departments to run daily business operations. It continues to evolve based on client feedback, utilizing the latest technology on the market. InnoSoft is the number one recreation software supplier for university and college Campus Recreation departments across the continent with over 180 university and college customers in Canada and the US.

This project will focus on the implementation of the Fusion recreation management system. The preferred approach for the University of Victoria will be to host the solution on-premises in the UVic Enterprise Data Centre. Professional Services staff from InnoSoft will be engaged to assist with both the functional and technical implementation of the system.

Much like the current CLASS system, this system will collect and store the personal information of Vikes Athletics and Recreation members, including students, staff, faculty, alumni and community members. The purpose of this document is to establish what implications there are in terms of FIPPA related to the implementation of this system.

## 1.2 Use of System

An installation of Fusion is based on the following 3-tier deployment architecture:

1. Database Tier
2. Application Tier
3. Client Tier

For additional technical details regarding the 3-tier deployment architecture, please refer to Appendix C.

The Fusion recreation management software (Client Tier) consists of the following two components:

1. **Smart-Client Desktop Application**: an employee-facing interface that is used throughout each recreation facility to manage all in-person processes (i.e. facility access, equipment checkout, in-person sales etc.).
2. **Web-Based Member Portal**: an online, customer-facing storefront that is used by customers to access online services and purchase items (i.e. register for programs, view facility availability etc.).

**Smart-Client Desktop Application**

The Fusion Smart-Client runs on Windows workstations (Windows 7, 8, 10) and is built using the Microsoft .NET Framework. ClickOnce deployment technology enables self-updating Windows-based applications that can be installed and run with minimal user interaction.

Vikes Athletics and Recreation staff members will use the Fusion Smart-Client to manage daily business operations, including:

- Facility rentals & bookings
- Accounts & program registration
- Program maintenance
- League management
- Memberships
- Point of sale (POS)
- Accounting
- Reporting
- Marketing and communications
- Equipment lending
- Access control and waivers

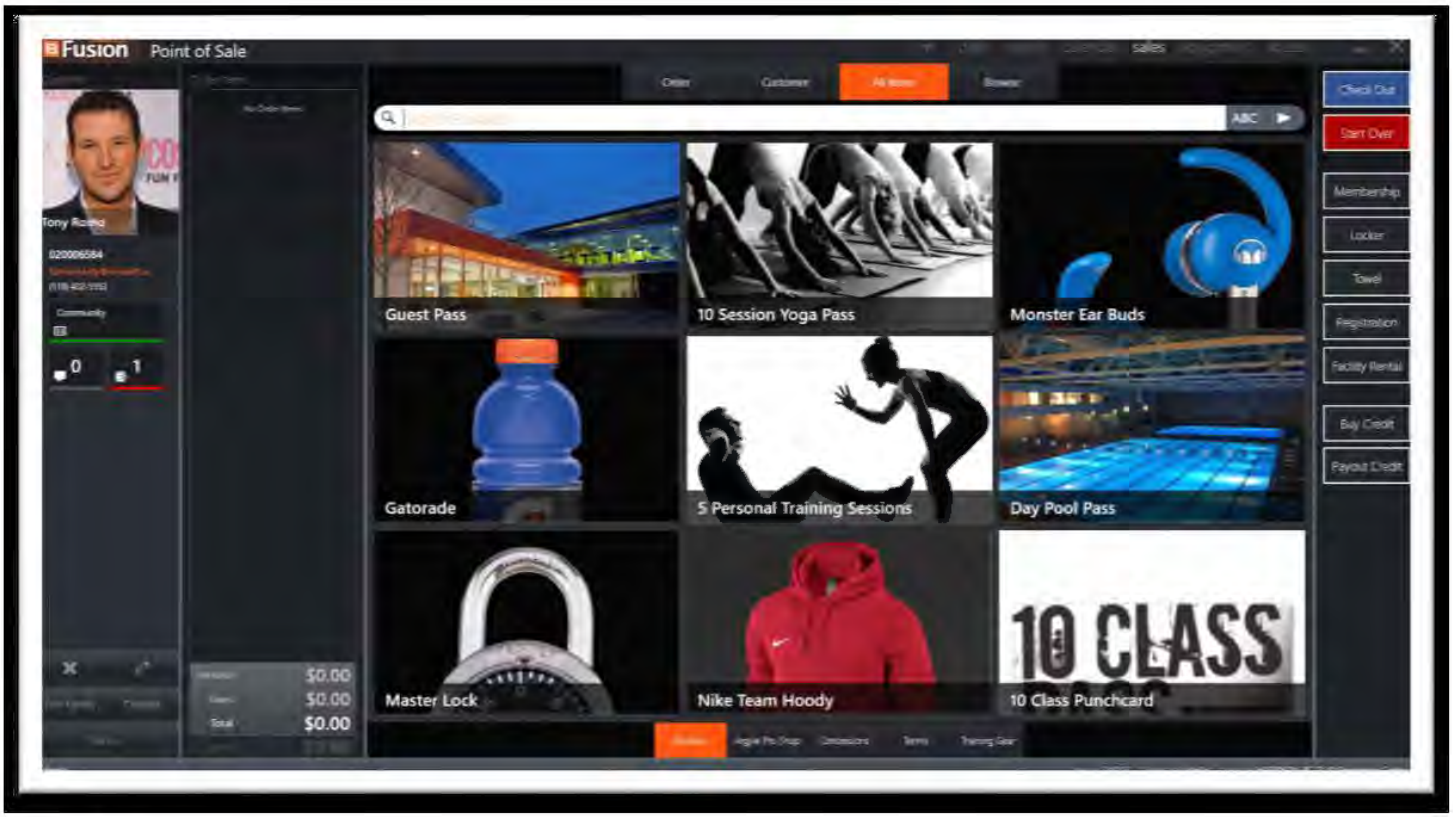



Figure 1. Fusion Desktop Application

**Web-Based Member Portal**

Fusion will allow members of the University community and the public to:

- Create an account with Vikes Athletics and Recreation
- Purchase memberships
- Register for recreation programs and leagues
- Book ATRS facilities
- Purchase items (Point of Sale)
- Borrow sports equipment
- Receive Vikes marketing and communications (optional based on customer preferences)

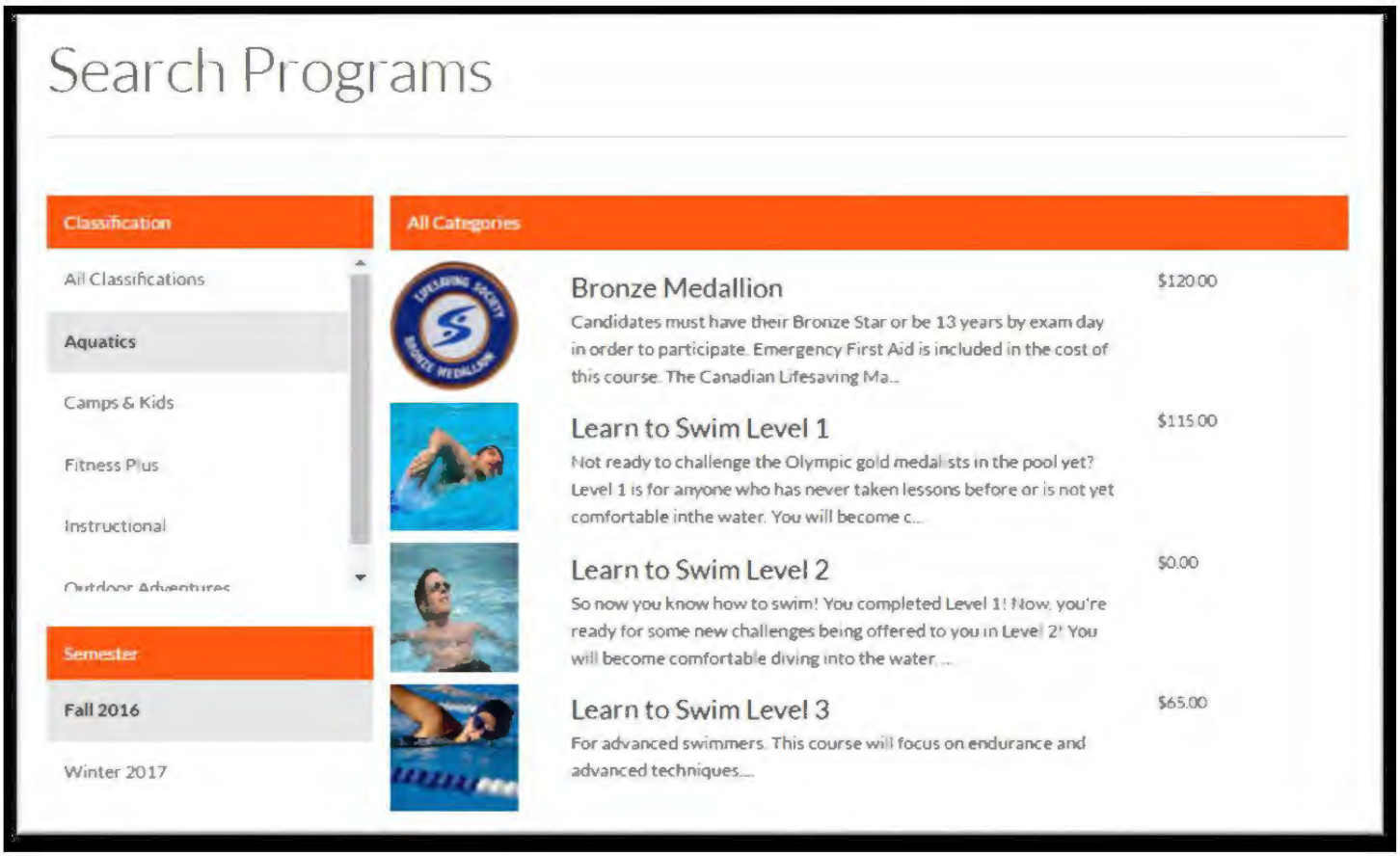



Figure 2. Fusion Member Portal

## 1.3 Custody and Control

The University will self-host Fusion on-premises in the Enterprise Data Centre and deploy a hosted environment based on InnoSoft's recommended server configuration documentation. **The University will have complete custody and control over the data that is imported and/or entered into the Fusion application. No data will be stored outside of Canada or in the public cloud.**

The scope of FIPPA applies to any records in the custody or control of the public body. The University will only maintain custody or control as contemplated in FIPPA over those records that are created as a function of the University's use and implementation of Fusion.

In addition, under section 26, the University of Victoria will collect personal information as it relates to the administrative activities of the public body and use that information only for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose; and if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use.

The information collected relates directly to and is necessary for the operation of recreation and varsity programs by Vikes Athletics and Recreation at its facilities. Personal information will be imported into Fusion from the Banner ERP system if an individual has recreational entitlement or if an individual provides their personal information for the purpose of creating an account. Full-time regular employees are eligible to access recreational facilities as part of their employment compensation and benefits. Students who pay athletics and recreation fees with their tuition are also eligible to access recreational facilities. Community members will be able to request creation of an account in-person or create an account online (if online account creation is enabled) using the Fusion member portal that will be hosted by the University.

In addition, use of Fusion is subject to the policies and guidelines listed below:

- Acceptable Use of Electronic Information Resources Policy
  http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf
- Protection of Privacy Policy
  http://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf
- Records Management Policy
  http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf
- Information Security Policy
  http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf
- Purchasing Services Schedule 3-6 Privacy Protection Schedule (to be attached to contract)
- http://www.uvic.ca/purchasing/assets/docs/PATRIOT%20ACT%20Provisions-Agreements-Privacy%20Protection%20Schedule.pdf
- InnoSoft Privacy Policy:
  http://www.innosoftfusion.com/privacy.php
- InnoSoft Terms of Use:
  http://www.innosoftfusion.com/terms.php

System users (clients/members) will participate and control their personal information as dictated by the University's policies. The University of Victoria will define what information is to be collected (i.e. member record creation, additional information collected during course or program registration etc.). The sharing and destruction of this data will be the responsibility of the University.

The University will define all limits on information collection, use and disclosure. Please note, if the University elects to NOT collect certain data (i.e. date of birth) certain system functionality may be compromised (e.g. program age restrictions).

In compliance with FIPPA and as stated in Section 30, personal information in the custody and control of the University of Victoria will be protected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal. If the University wishes to collect and store sensitive information, it can choose to configure Fusion's field-level encryption feature on sensitive data fields. Each designated field is encrypted using Sec. 15 The entire Fusion database can be encrypted at rest using Sec. 15 Sec. 15 (which supports Transparent Data Encryption). The University will utilize its most preferred/secured data transfer method to transmit University data (campus customer import files) to the hosted environment (e.g. SFTP or SSH). Additionally, appropriate Sec. 15 will be used to secure data in transit.

Significant product releases are available approximately once a quarter, and are preceded by release notes outlining the changes, additions and improvements made to the Software. InnoSoft's team members are certified and follow industry best practices and methods in secure development of the Fusion application (OWASP, Veracode testing etc.). InnoSoft will continue to monitor publications similar to OWASP 10 and will address any security updates and/or recommendations as they are made available. Additionally, database structuring follows Sec. 15

University system administrators will be responsible for maintaining User's roles/privileges/access. Fusion provides administrative users with the ability to define and assign security roles to subordinate users. Each security role then determines what system functionality each user has access to as soon as he/she logs in to the application. For example, a part-time student employee can be restricted from scheduling facilities, processing refunds, viewing sensitive demographic data etc. An unlimited number of custom security roles can be created and managed, allowing administrative users to layer system access appropriately based on different departmental roles.

Fusion provides a "Password Policies" configuration area that provides an administrative user with the ability to set and change complexity requirements (i.e. minimum length, is non-alpha required etc.) for both application and web user accounts. Fusion is also compatible with campus LDAP / Active Directory authentication as well as Shibboleth or CAS single sign-on services. Deploying one these integrations will allow users to access the Fusion member portal with existing campus credentials (i.e. without creating a web account). LDAP/AD integration can also be used to control employee access to the desktop application. Once an employee is successfully authenticated, his/her level of access to the application is controlled by the security role(s) assigned to the account.

The majority of system events, such as user access attempts, system alterations and transactions are tracked within a thorough audit process. Some of these events are displayed directly within the Fusion UI (i.e. user login history, facility scheduling history etc.) whereas others are stored outside of the UI. Furthermore, various logs/events can be viewed within Fusion's reporting tool (i.e. zero-dollar membership sales, refunds, facility access history etc.). Access to any stored log/audit trail that is not displayed within the system can be provided by the vendor if required.

During the implementation, it may be necessary to provide InnoSoft technical staff with temporary guided remote access using Remote Access Software (e.g. Remote Desktop over VPN connection or similar service) to servers that host Fusion to help install and configure the software. Additionally, upgrades may require temporary guided remote access for InnoSoft technical staff to be scheduled at the convenience of the University. Access is based on the University's rules and will only be allowed for the duration of the work being done.

The Contractor (InnoSoft) understands and agrees that the Contractor, including without limitation its agents, employees, and subcontractors, may, from time to time or to the extent necessary to carry out the Contractor's responsibilities under the contract, be exposed or have access to confidential data and/or information maintained by the University. The Contractor shall presume that all data and/or information received pursuant to the Contract is

confidential information and shall have a material duty to maintain the confidential character of such information unless otherwise designated by the University.

No confidential data collected, maintained, or used in the course of performance of the Contract shall be disseminated except as authorized by law and with the written consent of the University, either during the period of the Contract or thereafter. Any data supplied to or created by the Contractor shall be considered the property of the University. The Contractor must return any and all data collected, maintained, created or used in the course of the performance of the Contract, in whatever form it is maintained, promptly at the request of the University.

All InnoSoft employees are thoroughly screened before hiring. The screening process includes extensive reference checking and background checks. Only select InnoSoft technicians (Tier 2 & 3 technicians and developers) may access University data during the course of providing support and/or development resources to the customer. Any employee that has access to University data has been properly screened and trained. All access to these servers is closely monitored by the InnoSoft management team and audits are reviewed on a routine basis. No data will be taken offsite without the written consent of the University.

## 1.4 Personally identifiable information Data Types and Information Flows

Fusion allows staff and customers to create user accounts during which personal information is collected and stored in the database. Accounts are created in Fusion in several ways:

**Campus accounts:** are managed through a Sec. 15 Fusion provides a robust import interface that will be used to schedule and automate recurring imports of delimited files supplied by the ERP system. Each import routine is configured within Fusion to retrieve particular member files and update the Fusion database on a scheduled basis. The University will populate each data file with desired fields from the Banner ERP system that will then be imported into Fusion.

**Community accounts:** are created either online (if the University enables this feature) or in person with the assistance of a staff member. Existing community accounts may also exist in the system if obtained during the legacy import from CLASS. During online account creation, users are prompted to opt in or out of promotional email communication in accordance with Canada's Anti-Spam Legislation (CASL). During in-person account creation staff will toggle the option to opt in or out for the client.

**Organization accounts:** are created in person with staff or exist having been imported during the legacy import mentioned above.

**Family accounts:** are created by linking member records in the system (using “edit family” feature). The system does not create duplicate records for families, but rather simply links accounts (head of household, dependent, spouse etc.) to provide functionality to parents.

### Recurring Import Routines

A major aspect of implementation of Fusion is configuring an automated Sec. 15 routine between the ERP system and Fusion. The purpose of this automated import routine is to populate Fusion with campus-affiliated customers, their demographic data, and their membership and/or eligibility privileges.

Although the design of each import routine must follow some specific guidelines (i.e. file delimitation, field data format etc.), no specific template is utilized. Each institution’s data feed tends to be unique as the exact structure of each file depends on many factors (i.e. a client's business rules, desired fields and available fields).

The following fields are generally recommended:

- First Name
- Last Name
- Static ID Number (e.g. V-Number)
- Eligibility Flag (Student, Staff, Alumni, Retiree, etc.)
- Date of Birth
- Gender
- Email
- Phone
- Address
- Dynamic ID (Card Number)
- LDAP Username (NetLink ID)
- Academic Year
- Custom Fields

Each data element that is recommended (i.e. date of birth) is tied to one or multiple aspects of Fusion's functionality (i.e. pricing, restrictions, reporting etc.). Therefore, if particular data fields are not provided in the import routine (i.e. gender, date of birth etc.), the Recreation department may experience a degradation in Fusion's functionality (i.e. if date-of-birth is not provided, the department cannot offer age-specific pricing levels and/or enable age restrictions on electronic waiver acceptance).

## Customer Photos

Customer photos play a critical role in a client's operation of Fusion, as these photos are used to properly verify the identity of customers in a variety of situations (i.e. facility access, program check-in etc.). Each customer record in Fusion provides a placeholder for the customer's photo:


Figure 3. Customer Record with Photo

Traditionally, an existing campus photo directory is leveraged to populate Fusion with photos of each campus customer, as this eliminates the need to recapture photos of the entire campus population. Campus photos are not imported into Fusion though. Rather, they are referenced via one of the following supported interface methods:

1. **Directory Share:** an open share would be created between the campus photo directory and the Fusion Application Server via an application service account. The Fusion Application Server would then map through the photos to each client workstation (the photos would not reside in the application).
2. **Photos Downloaded to the Fusion Application Server:** photos would be transferred to the Fusion Application Server from the campus directory. These photos would then be "mapped" through to each client workstation (but would not reside in the application).
3. **Campus-Supplied RESTful Web Service:** a client can supply a RESTful web service that can be used to request each customer's photo as it is needed. Fusion supports the Sec. 15 and the Sec. 15 methods for security.
4. **InnoSoft-Supplied RESTful Web Service:** InnoSoft can supply a RESTful web service that can be used to request each customer's photo as it is needed. Fusion supports the Sec. 15 methods for security.

Although an interface with the central photo directory populates Fusion with the majority of the desired customer photos, the directory does not include photos of non-campus customers (i.e. Spousal Members, Community Members etc.), so new photos must be captured for these customers onsite at the recreation facility (typically via a webcam device). Only these new, captured photos are stored in the Fusion database as Binary Large Objects or BLOBs.

## Field Level Encryption

By default, Fusion automatically encrypts any data that is stored in the following two fields on each customer record:

- Medical Information
- Special Needs

These fields are often used to store important information that is collected from customers during program registration processes (i.e. the registrant could be prompted with "Do you have any allergies or medical concerns that we should be aware of?").

Custom fields can be added to keep track of any data Fusion does not track via standard fields (i.e. shirt size, certifications, etc.). Custom fields are often created by each client to enhance both registration functionality and reporting capabilities. Fusion's import tools can also be used to import data obtained from ERP systems into these user-defined custom fields.

To protect any sensitive data that is stored in these custom fields, administrators can enable field-level encryption on any field. This encryption is available with or without the utilization of TDE and SSL. Encryption for custom fields and prompts is accomplished using the Sec. 15 in the business layer.

## Authentication / Single Sign-On

A number of authentication and single sign-on interfaces can be deployed in order to secure customer authentication to the online Fusion member portal as well as user authentication to the Fusion desktop application.

**User Authentication**

An integration with existing LDAP/AD, Shibboleth or CAS authentication/SSO services will be deployed to control employee access to the desktop application. Once an employee is successfully authenticated, his/her level of access to the application is controlled by the security role(s) assigned to the account.


Figure 4. User Authentication to Desktop App

**Customer Authentication**

An integration with existing LDAP/AD, Shibboleth or CAS authentication/SSO services will also be deployed to control customer access to the Fusion member portal. Deploying one these integrations will allow client-affiliated customers to access the Fusion member portal with existing credentials (i.e. without creating a web account).

Sec. 15

**Local Authentication**

Fusion also provides embedded credential management functionality that can be used to support dual authentication methods for either user and/or customer sign in. For example, dual authentication can be deployed within the online member portal to allow non-affiliated customers to log in using Fusion-managed credentials, and allow affiliated customers to log in via credentials managed by the client (i.e. through Shibboleth). A "Password Policies" area is provided within Fusion's credential management component that allows administrators to set and change password complexity requirements (i.e. minimum length, is non-alpha required etc.) for both application and web user accounts.


Figure 6. Dual Authentication Example

## Security Roles

Fusion provides extensive role-based security options that can be used to configure an unlimited number of security roles. Each security role contains a granular list of functions and data that a user can be restricted from accessing. Once a security role has been defined by an administrative user, it can be assigned to an unlimited number of subordinate user records. A user can also possess multiple security roles (i.e. "Facilities Clerk" and "Front Desk Clerk").

## Data in Transit

Sec. 15 protect data in motion between servers and clients. This will encrypt the data and ensure that sensitive data cannot be viewed by eavesdroppers by means of network monitoring software. Sec. 15 also protects data integrity and prevents deliberate (malicious) modification of data while in transit.


Figure 7. SSL Communication Path

## Optional Database Encryption

Although not commonly utilized, a copy of Sec. 15 can be supplied by a client to encrypt the entire Fusion database at rest. The Enterprise edition of Sec. 15 provides full database level encryption in the Sec. 15 encrypts data in real time during file input and output. Sec. 15 Sec. 15

## Legacy Data Import

The legacy import of data from CLASS into Fusion is completed during the implementation process. Fusion's import tools allow you to assign a specific membership during each import process. This feature will be used heavily throughout this conversion process as it will allow you to assign memberships "en masse" to existing customers. During implementation InnoSoft's technical lead will provide University staff with documentation on the legacy import process. University staff will prepare the appropriate files and the import will be completed with the assistance of the technical lead. InnoSoft does not work with third parties or subcontractors. File preparation will be completed on premise by University staff and imported directly into the Fusion database.

## PCI Compliance

Fusion does not store or process any credit card information directly and will be able to meet the University's requirement for SAQ-A level PCI compliance. For online transactions, the system is designed to perform a complete redirect from the Fusion Web Portal to a third party payment gateway Sec. 15 and a redirect back from the third party payment gateway to Fusion. I-frames are not used. During the redirect, Fusion sends the transaction amount and order number to the Sec. 15 sends an authorization message back to Fusion which contains the order number. All elements of the payment pages delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider. For card-present transactions, PCI compliant third party credit card processing terminals will be setup such that there will be no integration between Fusion and the terminals. Payment amounts will be entered into both Fusion and the PCI compliant third party credit card processing terminals but any credit card information will be transacted through the PCI compliant third party credit card terminals only.

## Facility Access Controls

A dedicated access control interface will be used to monitor member access to any recreation facility and configured to suit the needs of the University's recreation department. This interface presents a variety of information to users including each member's photo, membership type, forgot card count and access violation messages. Fusion will automatically check a client's membership status each time they attempt to enter the facility (scanning/swiping their card, manual look up etc.). If the client possesses a membership which is valid for that facility or area they will be allowed to enter. In the event that the client does not possess a valid membership, staff will be notified by a visual warning as well as an optional audible warning. Turnstiles will not open for a client without a valid membership. Holders of campus cards will utilize their existing cards with Fusion using magnetic stripe readers. Fusion can track up to three different ID types on a member profile. Fusion supports both ID card printers and web cameras for the capture of photos and printing of cards onsite.

## Waivers and Liability Forms

Fusion allows for the creation and management of an unlimited number of waivers and liability forms in the system. It provides functionality that allows for acceptance of contract/waiver documents to be captured and tracked electronically. Waiver/contract documentation can be associated with any program or membership type. This documentation will be presented to customers during both in-person and online sales process. For in-person acceptance, contract/waiver documentation is pushed out to secondary capture devices (any device equipped with a web browser) and customers enter their signatures electronically via touch technology. For online acceptance, a customer can acknowledge acceptance through signature capture (using touch technology or a conventional mouse) or "click to accept". All accepted documents are stored indefinitely on each customer's profile. Staff may configure memberships to remain inactive until the appropriate waiver has been completed, blocking the member from facility access. Vikes Athletics and Recreation currently uses a waiver system linked to the UVic "My page" that is integrated

with CLASS. The implementation team will decide whether to integrate the existing waiver system or to use the waiver functionality that is built into Fusion.


Figure 8. InnoSoft Suggested Client Deployment Model

## 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>[Y/N]<br>[Date]</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.<br>See University Policy IM7800 for detailed definitions.<br>☐Highly Confidential<br>☒Confidential<br>☐Internal<br>☐Public<br>☐Don't Know<br>☐Information is not collected, maintained, or shared in any identifiable form as part of this project or service</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.<br><br>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.<br><br>
<table>
<tr><td>Highly Confidential</td><td>• [[Add a new bullet point for each data element]]</td></tr>
<tr><td>Confidential</td><td>• First Name<br>• Last Name<br>• Static ID Number (e.g. V-Number)<br>• Eligibility Flag (Student, Staff, Alumni, Retiree, etc.)<br>• Date of Birth<br>• Gender<br>• Email<br>• Phone<br>• Address<br>• Dynamic ID (Card Number)<br>• LDAP Username (NetLink ID)<br>• Academic Year<br>• Photo<br><br>In addition to the above types of personally identifiable information, there may be other information collected during registration that is critical to the safe operation of certain activities. This may include allergy information, special needs, and certifications. This information may be collected during the registration process.</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?</td><td>N</td></tr>
</table>

| | | |
|---|---|---|
| | [[If so, what are those technologies?<br>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.)]] | |
| 6 | **Will the project involve the collection or creation of new information about individuals?**<br><br>Similar to the existing Class system, the software will collect information about individuals who create an account to register for programs or memberships. Information collected will include first name, last name, email, birth date, gender, and photo. For the general public, this information will be collected in person at the front counter or online. For students, staff and faculty who qualify for recreation entitlement, this information will be imported daily from Banner and will also include V-Number and affiliation. | Y |
| 7 | **Will personal information about individuals or sensitive/critical information be disclosed to organizations, programs, processes or people who have not previously had routine access to the information?**<br><br>[[If so, which organizations, processes or people?]] | N |
| 8 | **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**<br><br>[[If so, how?]] | N |
| 9 | **Will the project collect, use, or disclose PII or sensitive/critical information for research purposes?**<br><br>[[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?**<br><br>[[If so, how may they perceive it to be intrusive?]] | N |
| 11 | **Is any of the information owned by another organization?**<br><br>[[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?**<br><br>[[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?**<br>[1-1000],[1001-5000],[5,001-50,000],[50,001-100,000],[100,000+] | Sec. 15 |
| 15 | **Where will the information be stored?**<br><br>The information will be stored in the UVic Data Centre. | |
| 16 | **Will a third party (e.g. vendor or service provider) have access to the information?** | Y |

| | | |
|---|---|---|
| | InnoSoft may require occasional temporary guided access to the database to provide support or to assist with upgrades. If temporary access is required, it will be monitored and disabled once the vendor has completed their tasks. | |
| **17** | **Is any of the information being accessed from outside of Canada?**<br><br>[[If so, by whom and from where?]] | **N** |
| **18** | **Does the IT system connect, receive, or share information in identifiable form, or PII or sensitive/critical information with any other IT systems?**<br><br>PII will be imported from the Banner ERP system Sec. 15 file will be created using a scheduled batch process and then saved to a secure network location. Photos will also be accessed over the UVic network. Sec. 15 Sec. 15 will be used to secure and limit access. | Y |
| **19** | **If there is external sharing, is it pursuant to new or existing information sharing agreements?**<br><br>[[List these agreements]] | **N/A** |

## 3.0 Privacy & Security Risks

| 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 | 2 | System users (clients/members) will participate and control their personal information as dictated by the University's policies. The University of Victoria will define what information is to be collected (i.e. member record creation, additional information collected during course or program registration etc.). The collection, use or disclosure of this data will be the responsibility of the University. |
| 2 | Unauthorized collection of PII by authorized individuals/processes/systems | 1 | 2 | System users (clients/members) will participate and control their personal information as dictated by the University's policies. The University of Victoria will define what information is to be collected (i.e. member record creation, additional information collected during course or program registration etc.). The collection, use or disclosure of this data will be the responsibility of the University. |
| 3 | Excessive collection of PII by authorized individuals/processes/systems | 1 | 2 | All efforts will be made to reduce the amount of PII required for the use of Fusion. Only the minimum required data will be migrated from CLASS and imported from the University's ERP system (Banner) that is required to provide services to members. |
| 4 | Inappropriate or unauthorized use of PII by authorized individuals/processes/systems | 1 | 2 | Personal information in the custody and control of the University of Victoria will be protected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal. |
| 5 | Unauthorized disclosure by individuals/processes/systems | 1 | 2 | Personal information in the custody and control of the University of Victoria will be protected by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal. |
| 6 | Creation of new PII by data matching | 1 | 2 | All efforts will be made to avoid the creation of new PII through data matching. Fusion may interconnect and share PII with other internal systems to support critical business processes including the automated account import from Banner, online waivers (if integrated with UVic My page), and the export of financial data for UVic Accounting Services. |
| 7 | Unauthorized tracking of individuals through transaction monitoring | 1 | 2 | SSL will be enabled to protect data in motion between servers and clients. This will encrypt the data and ensure that sensitive data cannot be viewed by eavesdroppers by means of network monitoring software. Utilizing SSL certificates also protects data integrity and prevents deliberate (malicious) modification of data while in transit. |

| | | | | |
|---|---|---|---|---|
| 8 | Data stored outside of Canada and in the public cloud | 1 | 2 | The University will self-host Fusion on-premises in the Enterprise Data Centre and deploy a hosted environment based on InnoSoft's recommended server configuration documentation. The University will have complete custody and control over the data that is imported and/or entered into the Fusion application. No data will be stored outside of Canada or in the public cloud. |
| 9 | Data retention beyond prescribed timeline | 2 | 2 | All data is stored indefinitely unless the University requests a purge of specific data elements (i.e. old customer records). Records are protected by security privileges within Fusion. Administrators may assign the privilege of member record viewing to specific individuals. Specific areas of the member record may also be protected by security privilege (i.e. medical information, special needs). |
| 10 | Risk of increased surveillance | 2 | 2 | The majority of system events, such as user access attempts, system alterations and transactions are tracked within a thorough audit. New employees will be informed that their actions in the system may be logged as part of their training and issuing their logon access. |
| 11 | Unauthorized use as a records repository | 2 | 2 | Fusion could be used as records repository as it provides the ability to upload documents to the system such as waivers, liability forms and rental contracts. The University will have complete custody and control over the data that is imported and/or entered into the Fusion application. No data will be stored outside of Canada or in the public cloud. |
| 12 | Public perception | 1 | 2 | The University will self-host Fusion on-premises in the Enterprise Data Centre and deploy a hosted environment based on InnoSoft's recommended server configuration documentation. The University will have complete custody and control over the data that is imported and/or entered into the Fusion application. No data will be stored outside of Canada or in the public cloud. |
| 13 | Use of existing PII data in a new system or business process | 3 | 1 | All efforts will be made to reduce the use of existing PII in a new system or business process. Fusion may interconnect and share PII with other internal systems to support critical business processes including the automated account import from Banner, online waivers (if integrated with UVic My page), and the export of financial data for UVic Accounting Services. |

# Consultation Checklist

## IT Projects

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

| Service Area | Impact? (Y/N) | Leader | Expert Consulted | Date of Consultation |
|---|---|---|---|---|
| Office of the CIO | | Wency Lum | | |
| Systems General Office | | Chandra Beaveridge | | |
| Client Technologies | | Lance Grant | | |
| Desktop Support Services | Y | David Street | David Street | July 10, 2017 |
| Computer Help Desk | | Marcus Greenshields | | |
| Academic & Admin Services | Y | Nav Bassi | Nav Bassi | July 7, 2017 |
| Client Account Managers | | Scott Thompson | | |
| Production and Technical Support | Y | Rizwan Bashir | | |
| Development Services | Y | Scott Thompson | | |
| Identity Services | Y | Corey Scholefield | | |
| UVic Online | Y | Scott Thompson | | |
| Data Centre Services | Y | Kim Lewall | | |
| Network Services | Y | Jane Godfrey | | |
| Infrastructure Services | | Ron Kozsan | | |
| Information Security Office | Y | Lance Grant | | |
| Project Management Office | | Chandra Beaveridge | | |

## Sponsor

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

| Name | Comments | Date of Consultation |
|---|---|---|
| **Michelle Peterson** | This is a thorough capture of the system, how it will be used, identified risks and risk mitigation | July 12, 2017 |

## Other Projects

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

| Department/Unit | Leader | Expert Consulted | Date of Consultation |
|---|---|---|---|
| | | | |
| | | | |

## Revision History

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

| Version | Date | Author | Comments |
|---|---|---|---|
| **1.0** | July 6, 2017 | Jan Misovic | DRAFT |

# Appendix A – Privacy Controls

| ID | PRIVACY CONTROLS |
|---|---|
| **AP** | **Authority and Purpose** |
| **AP-1** | **Authority to Collect**<br><br>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.<br><br>**Response:**<br><br>GV0235 Protection of Privacy Policy, section(s) 18.00, 19.00 |
| **AP-2** | **Purpose Specification**<br><br>The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 16.00, 17.00 |
| **DM** | Data Minimization and Retention |
| **DM-1** | **Minimization of Personally Identifiable Information**<br><br>Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;<br>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.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 19.00 |
| **DM-2** | **Data Retention and Disposal**<br><br>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;<br>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<br>Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 20.00, 25.00 |
| **DM-3** | **Minimization of PII Used in Testing, Training, and Research**<br><br>Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and<br>Implements controls to protect PII used for testing, training, and research<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 20.00, 21.00, 22.00 |
| **IP** | **Individual Participation and Redress** |

| ID | PRIVACY CONTROLS |
|---|---|
| IP-1 | **Consent**<br><br>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;<br>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;<br>Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and<br>Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 18.00 |
| IP-2 | **Individual Access**<br><br>Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 29.00, 32.00 |
| IP-3 | **Redress**<br><br>Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and<br>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.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 30.00, 31.00, 33.00 |
| IP-4 | **Complaint Management**<br><br>The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, section(s) 34.00 |
| **SE** | **Security** |
| SE-1 | **Inventory of Personally Identifiable Information**<br><br>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<br>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**<br><br>Develops and implements a Privacy Incident Response Plan; and<br>Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.<br><br>**Control(s) / Compliance:**<br><br>GV0235 Protection of Privacy Policy, Procedures for responding to a Privacy Incident or Privacy Breach |
| **UL** | **Use Limitation** |
| **UL-1** | **Internal Use**<br><br>The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.<br><br>**Control(s) / Compliance:**<br><br>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**<br><br>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;<br>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;<br>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<br>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.<br><br>**Control(s) / Compliance:**<br><br>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**<br><br>**Control:**<br><br>• Identifies and selects the following types of information system accounts to support organizational missions/business functions: organization-defined information system account types;<br>• Assigns account managers for information system accounts;<br>• Establishes conditions for group and role membership;<br>• 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;<br>• Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;<br>• Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;<br>• Monitors the use of information system accounts;<br>• Notifies account managers:<br>  • When accounts are no longer required;<br>  • When users are terminated or transferred; and<br>  • When individual information system usage or need-to-know changes;<br>• Authorizes access to the information system based on:<br>  • A valid access authorization;<br>  • Intended system usage; and<br>  • Other attributes as required by the organization or associated missions/business functions;<br>• Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and<br>• Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.<br><br>**Response:**<br><br>• Account Management is governed by the following institutional policies and procedures:<br>  • IM7200 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf<br>  • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf<br>• Account Management is subject to the operating procedures and processes of the University.<br><br>[[Add additional relevant information as required.]] |
| AC-3 | **Access Enforcement**<br><br>**Control:**<br><br>• The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.<br><br>**Response:**<br>• See AC-4, SC-7<br>[[Add additional relevant information as required.]] |

| ID | SECURITY CONTROLS |
|---|---|
| AC-4 | **Information Flow Enforcement**<br><br>**Control:**<br><br>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.<br><br>**Response:**<br><br>• See SC-7<br><br>[[Add additional relevant information as required.]] |
| AC-8 | **System Use Notification**<br><br>**Control:**<br><br>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.<br><br>**Response:**<br><br>• Organization-defined systems use policy will:<br>  • Primarily positive and explanatory (and not just a list of "don'ts").<br>  • Encourage usage by providing positive examples and suggestions.<br>  • Require that content be office-appropriate.<br>  • Require that personally identifiable information is not used.<br>  • Include links to University of Victoria policies and training resources<br><br>• Organization-defined systems use policy will include reference to and compliance with:<br>  • IM700 – Acceptable use of electronic information resources policy http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7200_6030_.pdf<br>  • GV0235 – Protection of Privacy http://www.uvic.ca/universitysecretary/assets/docs/policies/GV0235.pdf<br>  • IM7800 – Information Security and related procedures http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf<br>  • IM7700 – Records Management and related procedures, including Fair Dealings guidelines http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf<br>  • Canadian Copyright Act http://www.canlii.org/en/ca/laws/stat/rsc-1985-c-c-42/latest/rsc-1985-c-c-42.html<br><br>[[Add additional relevant information as required.]] |

| ID | SECURITY CONTROLS |
|---|---|
| AC-19 | **Access Control for Mobile Devices**<br><br>**Control:**<br><br>• Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and<br>• Authorizes the connection of mobile devices to organizational information systems<br><br>**Response:**<br><br>• University of Victoria recommends for all users and requires for Exchange users the use of:<br>  • Sec. 15<br>  •<br>  •<br>[[Add additional relevant information as required.]] |
| AC-20 | **Use of External Information Systems**<br><br>**Control:**<br><br>• 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:<br>  • Access the information system from external information systems; and<br>  • Process, store, or transmit organization-controlled information using external information systems.<br><br>**Response:**<br><br>• See CP-9, PE-3, SC-7, SI-8<br><br>[[Add additional relevant information as required.]] |
| AC-21 | **Information Sharing**<br><br>**Control:**<br><br>The organization:<br>• 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<br>• Employs organization-defined automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions.<br><br>**Response:**<br><br>• See AC-20<br><br>[[Add additional relevant information as required.]] |
| AC-22 | **Publically Accessible Content**<br><br>**Control:**<br><br>The organization:<br>• Designates individuals authorized to post information onto a publicly accessible information system;<br>• Trains authorized individuals to ensure that publicly accessible information dees 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<br>• Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.<br><br>**Response:**<br><br>• See AC-4, AC-21, IA-2, IA-8<br><br>[[Add additional relevant information as required.]] |
| **AT-2** | **Security Awareness Training**<br><br>**Control:**<br><br>• The organization provides basic security awareness training to information system users (including managers, senior executives, and confractors):<br>  • As part of initial training for new users;<br>  • When required by information system changes; and<br>  • Organization-defined frequency thereafter.<br><br>**Response:**<br><br>• Privacy training will be required for new users to ensure compliance with FIPPA.<br><br>[[Add additional relevant information as required.]] |
| **AU-6** | **Audit Review, Analysis, and Reporting**<br><br>**Control:**<br><br>The organization:<br>• Reviews and analyzes information system audit records for indications of defined inappropriate or unusual activity.<br>• Reports findings to the Chief Privacy Officer and Chief Information Officer<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **CA-3** | **System Interconnections**<br><br>**Control:**<br><br>The organization:<br>• Authorizes connections from the information system to other information systems through the use of interconnection Security Agreements;<br>• Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and<br>• Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **CM-3** | **Configuration Change Control** |

| ID | SECURITY CONTROLS |
|---|---|
| | **Control:**<br><br>The organization:<br>• Determines the types of changes to the information system that are configuration-controlled;<br>• Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;<br>• Documents configuration change decisions associated with the information system;<br>• Implements approved configuration-controlled changes to the information system;<br>• Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];<br>• Audits and reviews activities associated with configuration-controlled changes to the information system; and<br>• Coordinates and provides oversight for configuration change control activities through the: organization-defined configuration change control that convenes organization-defined configuration change conditions.<br><br>**Response:**<br><br>• System configuration settings and changes are managed using the University systems Change Management processes and Change Advisory Board (CAB).<br><br>[[Add additional relevant information as required.]] |
| **CM-8** | **Information System Component Inventory**<br><br>**Control:**<br><br>• Develops and documents an inventory of information system components that:<br>  • Accurately reflects the current information system;<br>  • Includes all components within the authorization boundary of the information system;<br>  • Is at the level of granularity deemed necessary for tracking and reporting; and<br>  • Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and<br>• Reviews and updates the information system component inventory.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **CM-10** | **Software Usage Restrictions**<br><br>**Control:**<br><br>The organization:<br>• Uses software and associated documentation in accordance with contract agreements and copyright laws;<br>• Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and<br>• Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **CP-2** | **Contingency Plan**<br><br>**Control:** |

| ID | SECURITY CONTROLS |
|---|---|
| | The organization develops a contingency plan for the information system.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **CP-9** | **Information System Backup**<br><br>**Control:**<br><br>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.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **IA-2** | **Identification and Authentication (organizational Users)**<br><br>**Control:**<br><br>• The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).<br><br>**Response:**<br><br>• See SC-8<br><br>[[Add additional relevant information as required.]] |
| **IA-8** | **Identification and Authentication (non-organizational users)**<br><br>**Control:**<br><br>• The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).<br><br>**Response:**<br><br>• See SC-8<br><br>[[Add additional relevant information as required.]] |
| **MP-2** | **Media Access**<br><br>**Control:**<br><br>• The organization restricts access to organization-defined types of digital and/or non-digital media] to personnel or roles.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **PE-3** | **Physical Access Control** |

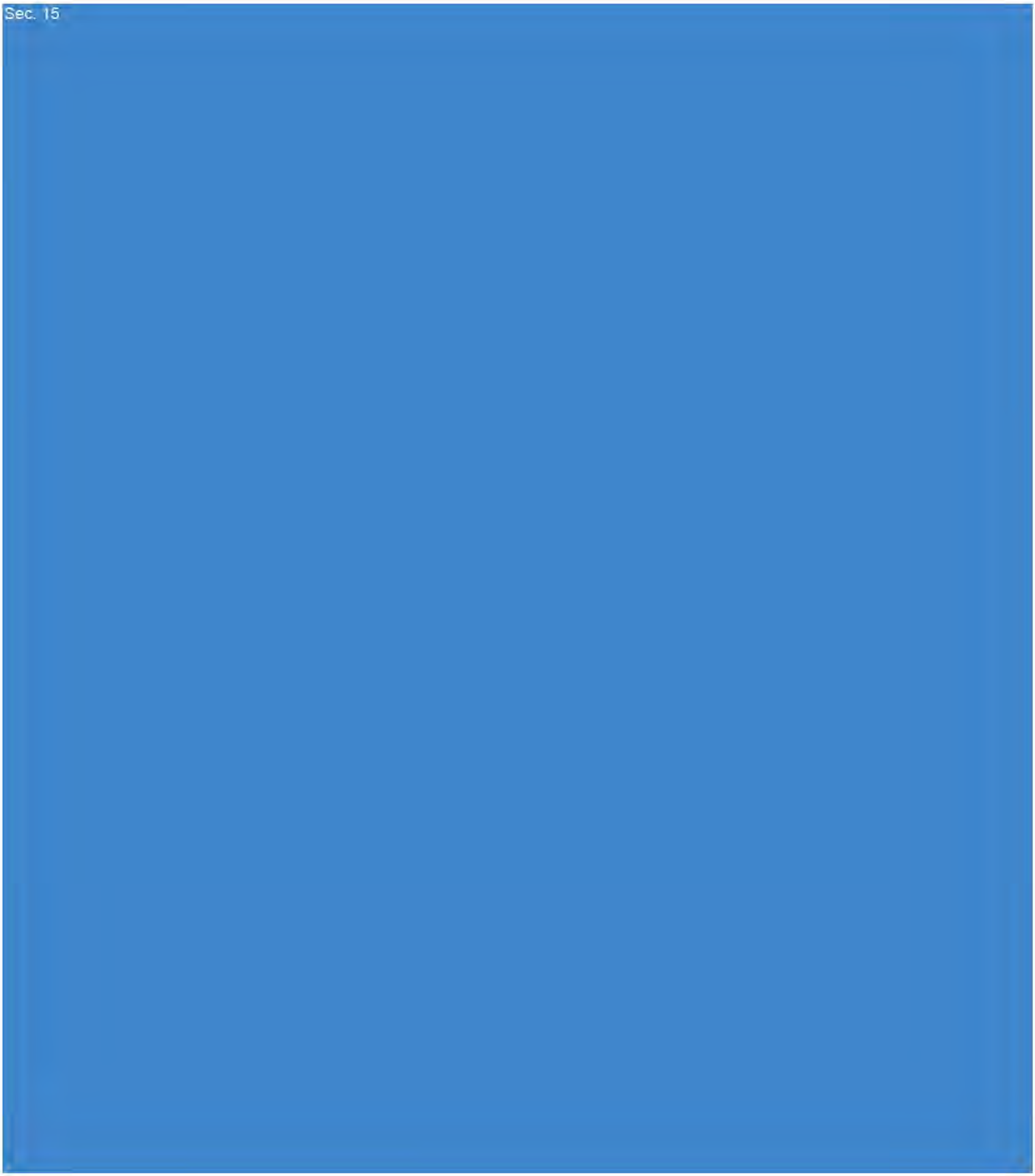
| ID | SECURITY CONTROLS |
|---|---|
| | **Control:**<br><br>• Enforces physical access authorizations, controls and audits exist.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| **PL-4** | **Rules of Behavior**<br><br>**Control:**<br><br>• Establishes and makes readily 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;<br>• 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;<br>• Reviews and updates the rules of behavior; and<br>• 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<br><br>**Response:**<br><br>• See AC-8, CM-10<br><br>[[Add additional relevant information as required.]] |
| **RA-3** | **Risk Assessment**<br><br>**Control:**<br><br>The organization:<br>• 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;<br>• Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];<br>• Reviews risk assessment results [Assignment: organization-defined frequency];<br>• Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and<br>• 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.<br><br>**Response:**<br><br>• See sections 1.4 and 3.0 of this document.<br><br>[[Add additional relevant information as required.]] |
| **SC-7** | **Boundary Protection**<br><br>**Control:**<br><br>• Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;<br>• Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and |

| ID | SECURITY CONTROLS |
|---|---|
| | • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| SC-8 | **Transmission Confidentially and Integrity**<br><br>**Control:**<br><br>• The information system protects the confidentiality and; integrity of transmitted information.<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| SI-8 | **SPAM Protection**<br><br>**Control:**<br><br>The organization:<br>• Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and<br>• Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures<br><br>**Response:**<br><br>[[Add additional relevant information as required.]] |
| SI-12 | **Information Handling and Retention**<br><br>**Control:**<br><br>• 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<br><br>**Response:**<br><br>• 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<br><br>[[Add additional relevant information as required.]] |

# Appendix C – Hosting Architecture

## Deployment Model

**An installation of Fusion is based on the following 3-tier deployment architecture:**


Sec. 15

## Firewall Rules

**The use of appropriate firewall rules is recommended in order to properly secure communication between client workstations and the Fusion hosted environment. Provided below are standard communication ports that are utilized (although these can be altered if need be):**

# Server Roles

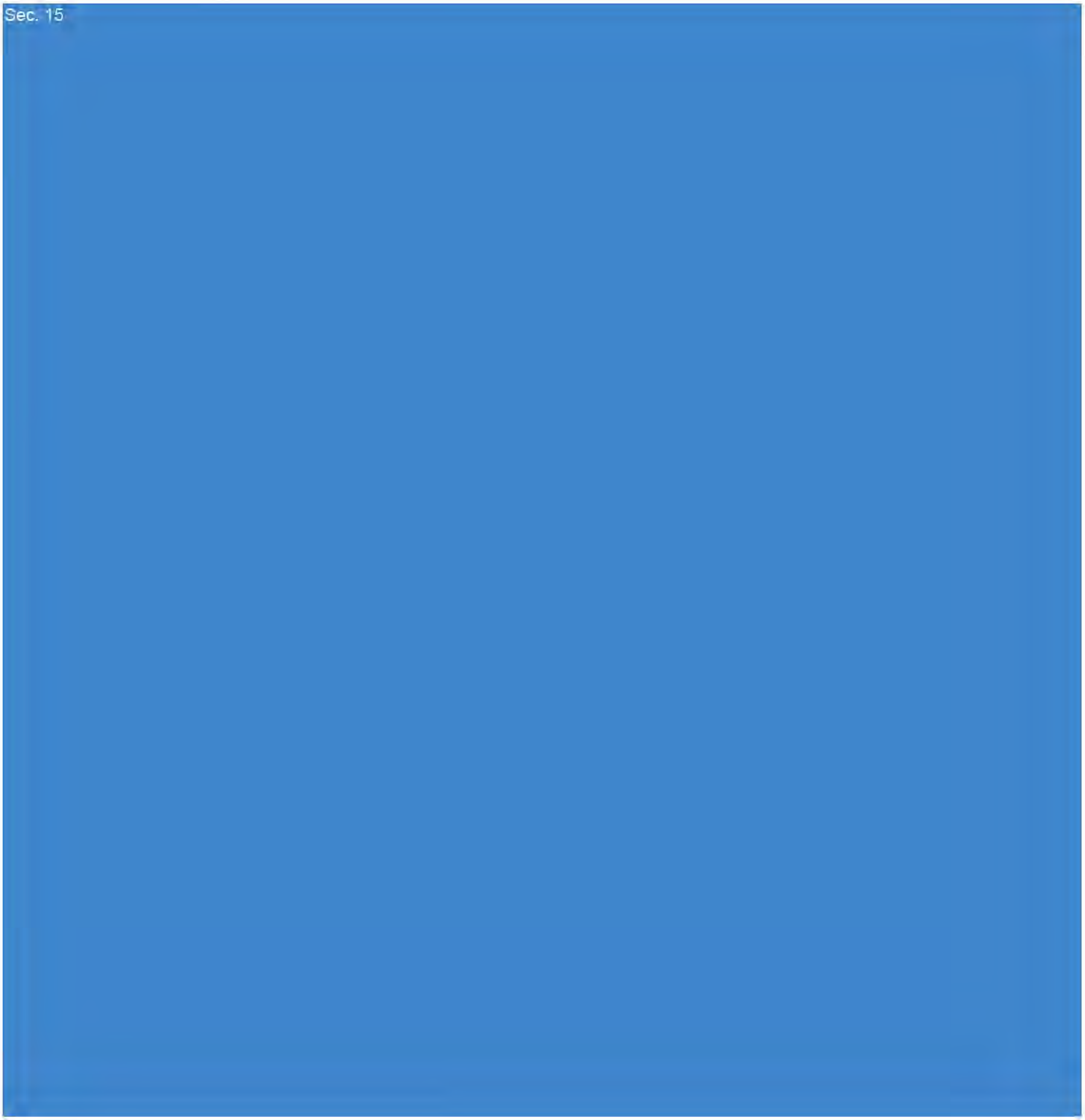
| | Application Server | Web Server |
|---|---|---|
| **Common HTTP Features** | | |
| Default Document | ✓ | ✓ |
| Directory Browsing | ✓ | ✓ |
| HTTP Errors | ✓ | ✓ |
| Static Content | ✓ | ✓ |
| **Health and Diagnostics** | | |
| HTTP Logging | ✓ | ✓ |
| **Performance** | | |
| Static Content Compression | ✓ | ✓ |
| Dynamic Content Compression | ✓ | ✓ |
| **Security** | | |
| Request Filtering | ✓ | ✓ |
| **Application Development** | | |
| .Net Extensibility 4.5 | ✓ | ✓ |
| ASP.NET 4.5 | ✓ | ✓ |
| **Management Tools** | | |
| IIS Management Console | ✓ | ✓ |

# Server Features

| | Application Server | Web Server |
|---|---|---|
| **.Net Framework 3.4 Features** | | |
| .NET Framework 3.4 | ✓ | ✓ |
| **.Net Framework 4.5 Features (all)** | ✓ | ✓ |
| **Message Queueing Services** | | |
| Message Queueing Server | ✓ | |
| **Windows Process Activation Service** | | |
| Process Model | ✓ | ✓ |
| .NET Environment 3.5 | ✓ | ✓ |
| Configuration APIs | ✓ | ✓ |

Application Server:

| HARDWARE/SOFTWARE | REQUIREMENTS |
|---|---|
| 64-Bit Operating System (in order of preference) | ∇ Windows Server 2016 (Recommended)<br>∇ Windows Server 2012 R2<br>∇ Windows Server 2012<br>∇ Windows Server 2008 R2 (Web or Standard Edition) |
| Processor | ∇ Quad Core 3.0 GHZ or faster recommended |
| Memory (RAM) | ∇ 6 GB or more recommended |
| Hard Disk | ∇ Must have sufficient disk resources for Operating System and other software requirements:<br>○ **Minimum space: 60GB**<br>○ **Recommended: 100GB or more** |
| Display | ∇ Admin tools require 1024x768 or higher resolution |
| Other Requirements | ∇ Internet Information Services (IIS)<br>∇ WCF Host<br>∇ Microsoft Message Queuing (MSMQ)<br>∇ .NET Framework 3.5 SP1 & 4.6<br>∇ Microsoft Point of Service for .Net v1.14<br>∇ Microsoft Enterprise Library 4.1<br>∇ Internet Software:<br>○ **Minimum Browser: IE10 or newest version**<br>○ **Recommended Browser: Chrome (newest version)**<br>∇ SQL Server Management Studio<br>∇ Remote Access Software for Fusion Technical Support:<br>○ **Remote Desktop.**<br>○ **VPN support if available.**<br>○ **FTP Client Software (must support SFTP):**<br>▪ Recommended: FileZilla. |


Sec. 15

Web Server:

Sec. 15