Privacy Impact Assessment (PIA)

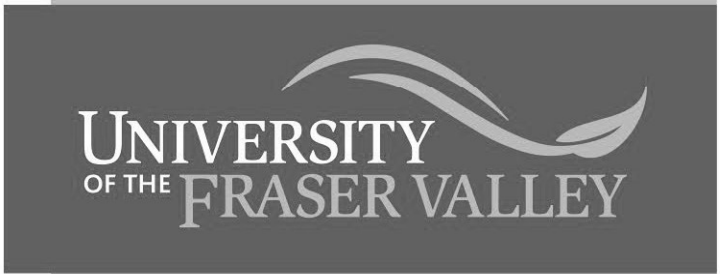
Version 0.3e

PIA Sygyzy Juypter

Program Manager:
Alex Diaz
Director of Infrastructure and Operations,
Office of the Chief Information Officer

Author:
Crawford Millen
Director of Information Security
Office of the Chief Information Officer

Date:
2021-04-28



Version History

Ver	Date	Author	Description
0.1	2021-04-28	s. 22	
0.2	2021-05-13		
0.3			
0.4			
0.5			
0.6			
0.7			
0.8			
0.9			
1.0			
1.0b			

Table of Contents

Part 1 – General

Name of Department/Branch:	Information Technology Services		
PIA Drafter:	Crawford Millen		
Email:	crawford.millen@ufv.ca		
Program Manager:	Alex Diaz		
Email:	Alexander.diaz@ufv.ca		

The objective of a Privacy Impact Assessment (PIA) is to determine how a program or service, could affect the privacy of individuals. It aims to identify and reduce any possible negative effects on privacy that might result from implementing a program or service. This specific PIA's objectives are first to determine if there are privacy issues or risks associated with the University of the Fraser Valley's proposed adoption of Microsoft Office 365 (M365); and if so, to provide recommendations and mitigation strategies. This will include identification of issues with compliance with regard to the *Freedom of Information and Protection of Privacy Act,* R.S.B.C. 1996, c. 165 ("FIPPA"), and determine how UFV can avoid or minimize the loss, damage, misuse or abuse of personal information.

In addition, this PIA is a way for UFV to demonstrate its commitment to protecting the privacy of individuals, promote transparency and accountability, and contribute to continued public confidence in the way that the University of the Fraser Valley (UFV) manages personal information. It helps prepare UFV to implement the project with proper consideration of relevant privacy requirements, including those privacy requirements in the architecture, design, and configuration.

This PIA is guided by the requirements laid out in FIPPA:

Section 69(5.3) of the Freedom of Information and Protection of Privacy Act (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA. Public bodies should contact the privacy office(r) for their public body to determine internal policies for review and sign-off of the PIA. Public bodies may submit PIAs to the Office of the Information and Privacy Commissioner for BC (OIPC) for review and comment.

This PIA also explains the process UFV followed, the factors considered, and the steps taken or will undertake to make sure this decision does not adversely affect the privacy of the UFV community. This undertaking is part of UFVs commitment to make careful and considered decisions in safeguarding the personal information of staff, students, and all other stakeholders. It explains our reasons for the move, the context within which we made the decision, the key privacy risks identified as potential barriers to cloud use, and the reasons these can be overcome.

This report is meant to aid information technology, information management, and access to information and privacy staff, along with the directors and executive directors, to be better informed about the risks, and recommend appropriate safeguards in order to securely transition to the cloud. It also assumes that the M365 A3 package will be used and thus all of its associated services are available to UFV. While the UFV initiative focuses on the implementation of Exchange Online, since this implementation will require both Azure Active Directory (AAD) and M365, therefore this PIA covers these technologies.

1. Description of the Initiative

JupyterHub on syzygy.ca is a computational service being provided since March 2017 by PIMS, in cooperation with ComputeCanada. A project of the *Pacific Institute for the Mathematical Sciences (PIMS)*, *Compute Canada* and *Cybera* "syzygy.ca" brings Jupyter notebooks to researchers, educators and innovators across Canada. The Syzygy service has been used by over 16,000 students at 20 universities across Canada. Working with the IT team at the University of the Fraser Valley, PIMS provides access to this service to groups of users at UFV including faculty and students.

Jupyter Notebook is an open-source web application that allows users to create and share documents that contain live code, equations, visualizations and narrative text. The service joins the mathematical sciences expertise from PIMS with the computational resources of Compute Canada to provide a service that responds to the need for an accessible computing platform for Canadian researchers. By delivering an easy-to-use scientific computing and data analysis environment through a web interface, the service lowers the barrier to code creation, data visualization and research collaboration. Uses include: data cleaning and transformation, numerical simulation, statistical modeling, data visualization, machine learning, and much more. Jupyter Hub is a multi-user version of the notebook designed for classrooms, researchers, and companies.

The syzygy computing service is an implementation of the Jupyter Hub on dedicated hardware accessible over the web. There is a great deal of information about Jupyter available at the Jupyter project site, http://jupyter.org/

s. 15(1)(l), s. 17, s. 21 [redacted]

s. 15(1)(l), s. 17, s. 21

2. Scope of this PIA

The scope of this PIA is centered on the UFV's adoption of Juypter Hub, a service provided by PIMS, in cooperation with ComputeCanada. The service is a project of the Pacific Institute for the Mathematical Sciences (PIMS), Compute Canada and Cybera. The technical details are aligned with documentation published on the project website at "https://github.com/pimsmath". The technical materials referenced are published on the PIMS github under the "syzygy-brochure" and "syzygy-infrastructure" repositories.

Within scope is the personal information data that flows between UFV's on-premises directory (AD), via ADFS single signon, and the Syzygy service being processed in the Compute Canada data centres.

The current intention is that this will be used by the faculty in the Department of Mathematics, to provide access to the service to assess if this will be relevant to, and possibly offered in courses. Later phases of adoption will have the service included in courses and offered to UFV students.

3. Related Privacy Impact Assessments

No other PIA issued by UFV are related or relevant to this project. This is the first PIA to cover the services being offered by the *Pacific Institute for the Mathematical Sciences ("PIMS")*, *Compute Canada* and *Cybera*.

4. Elements of Information or Data

This PIA uses the terms Contact Information (CI), Personal Identity Information (PII) and Personal Information (PI) as defined in Schedule 1 of the BC FIPPA.

"personal identity information" means any personal information of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual;
"personal information" means recorded information about an identifiable individual other than contact information;
"contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

To describe the data elements used in the initiative, we will describe the types of data used, who controls the data types, the flow of information, and the elements that can potentially hold CI, PI or PII data.

Data Types

With regard to the initiative covered in tis PIA, there are four types of information shared with, collected and used in delivering services:

- Diagnostic Data,
- Functional Data,
- Authentication Data,
- Customer Data.

Diagnostic Data is produced by system components for the purpose of maintaining and providing the service. While this may be produced by user activity, it is not customer information or generated content. Diagnostic Data is used to keep services secure and up-to-date, detect, diagnose and remediate problems, and facilitate product improvements. UFV defines Diagnostic Data as referring only to telemetry data collected about the specific use of software.

Functional Data is data that is necessary only for a short period of time, to communicate with services on the Internet, including UFV's own apps and services. Examples of Functional Data are the data stream necessary to allow the user to authenticate, SSL certificates, or verification of a valid service license. The key difference between Functional Data and Diagnostic Data is that Functional Data should be transient.

Authentication Data is used to facilitate authentication and identification of each user. This includes the user's userPersonalName (the user's login ID, referred to hereafter as "UPN"), the user's full name, and a authentication token.

Customer Content is user-created content which is defined as information in the user's profile, emails, calendar and other information that the user themselves decides to place into the service. This information is created by the user and may be personal, work-related, administrative, research or educational and may contain personal information that they place into the service.

Control of Data

Under the privacy requirements, *Diagnostic* and *Functional Data* meet the FIPPA conditions for:

33.2(1)(p.2) if the information is metadata that

(i) is generated by an electronic system, and

(ii) describes an individual's interaction with the electronic system,

and if,

(iii) if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and

(iv) in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;

Therefore, these data types do not have data that correlates with the definition of PI or PII contained under FIPPA (2019).

Data Elements

Object Types	Source	Comment
eduPersonPrincipalName	UFV AD	s. 15(1)(l)
eduPersonEntitlement	UFV AD	s. 15(1)(l)
puid	UFV AD	s. 15(1)(l)
mail	UFV AD	s. 15(1)(l)

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to your privacy office(r). They will guide you through the completion of your PIA.

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Storage

s. 15(1)(l)

Access

s. 15(1)(l)

6. Data Linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity

In FOIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	**YES**
2. Those services are provided through: (a) public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	**YES**
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	**NO**
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

With reference to the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165, (amended 2019), personal information processing between Microsoft and UFV can be performed as approved under the following stipulations for collection and disclosure:

S. 26(c) - Collection - the information relates directly to and is necessary for a program or activity of the public body,

S. 33.1(1) (p) if the disclosure

(i) is necessary for

(A) installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment that includes an electronic system, or

(B) data recovery that is being undertaken following the failure of an electronic system that is used in Canada, by the public body or by a service provider for the purposes of providing services to a public body, and

(ii) in the case of disclosure outside Canada, results in temporary access and storage that is limited to the minimum period of time necessary to complete the installation, implementation, maintenance, repair, trouble-shooting, upgrading or data recovery referred to in subparagraph (i); and

(p.1) if the disclosure

(i) is necessary for the processing of information and if that processing does not

(A) involve the intentional access of the information by an individual, or

(B) result in the storage of personal information, other than personal information that is metadata, outside Canada, and

(ii) in the case of disclosure outside Canada, results in temporary access that is limited to the minimum period of time necessary to complete the processing;

(p.2) if the information is metadata that

(i) is generated by an electronic system, and

(ii) describes an individual's interaction with the electronic system,

and if,

(iii) if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and

(iv) in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;

S. 33.2(c) - Disclosure - to an officer or employee of the public body or to a minister, if the information is

necessary for the performance of the duties of the officer, employee or minister;

s. 15(1)(l), s. 17

Personal Information Flow - Exchange			
#	Description/Purpose	Type	FIPPA
1	User authenticates s. 15(1)(l), s. 17	Use (by UFV)	s. 32(a)
2	s. 15(1)(l), s. 17, s. 21	Disclosure (to Syzygy)	s. 33.2(a)

9. Risk Mitigation Table

Risk	Pro-bability	Impact	Service Measure	UFV Measures
PI exposed though ADFS compromise.	LOW	MED	s. 15(1)(l), s. 17	s. 15(1)(l), s. 17, s. 21
PI exposed in transit.	LOW	MED	s. 15(1)(l), s. 17, s. 21	s. 15(1)(l), s. 17, s. 21
Perception of PI vulnerability	MED	LOW		a: Transparent communication of benefits and controls to stakeholders will assist in reassuring users UFV undertaking with focus of protecting PII. b: Will assist to ensure users are aware of how sensitive data should be managed.

10. Collection Notice

This service will not collect personal information and therefore there is no requirement to provide a collection notice.

Part 3 – Security of Personal Information

11. Please describe the physical security measures related to the initiative (if applicable).

Standards Compliance
The major international standards relevant to UFV's privacy requirements are:

- **ISO 27001 –** the International Standards Organization's comprehensive set of benchmarks includes a rigorous set of physical, logical, process and management controls defined by ISO 27001:2013;
- **ISO27018 -** code of practice for the protection of personal data in the cloud. Based on ISO security standard 27002 and provides implementation guidance on ISO27002 controls applicable to public cloud Personally Identifiable Information (PII).

Security Breach Protocols

s. 13, s. 15(1)(l)

12. Please describe the technical security measures related to the initiative (if applicable).

AUTHENTICATION

s. 15(1)(l), s. 17, s. 21

PERMISSIONS

s. 15(1)(l), s. 17, s. 21

Role Based Access Control (RBAC)

s. 15(1)(l), s. 17, s. 21

LOGGING

s. 15(1)(l), s. 17, s. 21

SUMMARY

s. 15(1)(l), s. 17, s. 21

13. Does your branch/department rely on any security policies?

UFV's ITS department respects the rights of users' privacy, in accordance with university policies and relevant legislation. As stated in the Universities Acceptable Use of Computer and Network Resources, UFV will not access a user's account unless they are investigating a case of system abuse or otherwise acting in accordance with FIPPA.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

s. 15(1)(l), s. 17

- s. 15(1)(l), s. 17, s. 21 [redacted]

15. Please describe how you track who has access to the personal information.

LEGAL DISCLOSURE

Access to personal data may occur at the request of law enforcement officials or due to a legal process (i.e. subpoenas). UFV has processes in place to carefully review, validate and respond to lawful access requests or other legal processes. The user may be notified of such access unless it would compromise the investigation or the law or court order prohibits such notification. Any access request received by UFV will be responded to in accordance with the requirements of FIPPA.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

s. 15(1)(l), s. 17, s. 21 . UFV can decide which attributes are passed to the service in the s. 15(1)(l), s. 17, s. 21, but generally, s. 15(1)(l), s. 17, s. 21 will be the sole source for all data and all changes to user attributes will be performed against this system.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

N/A

18. If you answered "yes" to question 16, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

19. If you answered "yes" to question 17, do you have records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact your privacy office(r).	NO

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact your privacy office(r).	NO

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

Personal Information Bank	
Personal Information Bank Name	n/a
Personal Information Bank Location	n/a
The purpose of the Collection, Use, and Disclosure of Personal Information	n/a
Authority for Collection of Personal Information	n/a

Collected Personal Information is About	n/a
Type(s) of Personal Information Collected will include	n/a
In accordance with FIPPA and other applicable laws and policies, personal information may be used by and/or disclosed to	n/a

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Privacy Office(r)/or individual responsible comments

This PIA is based on a review of the material provided to the Privacy Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to the Privacy Office(r).

Stephen Gaspar Legal Counsel University of the Fraser Valley	Signature	Date

Part 7 – Administrative Office(r)/or individual responsible comments

This PIA is based on a review of the material provided to the Administration Office(r) as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA Update and submit it to the Administrative Office(r).

Jackie Hogan Chief Financial Officer & VP Administration, University of the Fraser Valley	Signature	Date

Part 8 – Program Area Signatures

Steven Banyai Chief Information Officer, University of the Fraser Valley	Signature	Date
Crawford Millen Author/Director Information Security OCIO University of the Fraser Valley	Signature	Date
Jacqueline Toering Dir. Risk & Safety, University of the Fraser Valley	Signature	Date
Alex Diaz Dir. Infrastructure & Operations OCIO, University of the Fraser Valley	Signature	Date

A final copy of this PIA (with all signatures) must be kept on record.