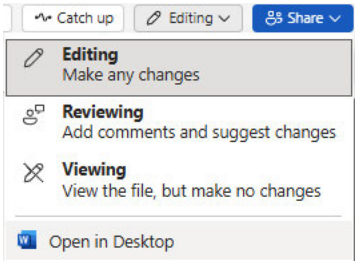
Privacy Impact Assessment for:

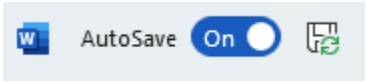
Unified Communications Program: OpenText Fax Solution

Initiative:	OpenText Fax Solution
Department or Service Area Name:	ITS

Tip: Consider using the Microsoft Word Desktop app for a better experience while completing this form.



Once in desktop, the file should be linked to the online version. Just ensure that the autosave toggle is enabled (upper left side of screen):



Part 1 – General Information and Overview

1.1 What is the Initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Implement a reliable cloud-based or network-based digital fax solution.

Ensure secure transmission of sensitive documents in compliance with BC's Freedom of Information and Protection of Privacy Act (FIPPA).

Decommission legacy analog fax machines where feasible.

Integrate the new fax solution with existing email and document management systems.

Provide comprehensive user training and support documentation for staff and faculty.

Achieve operational cost savings and reduce the university's environmental footprint (paper, toner, electricity).

1.2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA will assess VIU's use of OpenText as part of the Unified Communications Program (UCP). It does not cover how VIU staff and departments manage the records that they fax.

1.3. Are there any related Privacy Impact Assessments?

Please indicate if this an update on an existing PIA or an additional module that was not covered in the original PIA.

No

1.4. What are the data or information elements involved in your initiative?

In the table below, please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in an appendix.

Information Type	Information Collected
Personal Information	Various types of sensitive student/employee personal information such as health files, accessibility plans, dental records, student records, employee records, etc.
Contact details	
Account information: what info is required to set up an account?	
Commercial information	

1.4a. Did you list personal information in question 1.4?

Personal information (PI) is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference- see the table below for examples of Personal Information.

Business contact information, in turn, is defined as information to enable an individual at a place of business to be contacted and includes the name, position name or title, as well as business telephone number, address, email or fax number of the individual. BC FIPPA does not protect business contact information.

Examples of Personal Information	
1. Name, age, sex, weight, height 2. Home address, phone number 3. Race, ethnic origin, sexual orientation 4. Medical information 5. Health history 6. Number or symbol assigned to the individual 7. Income, purchases and spending habits 8. Blood type, DNA code, fingerprints	9. Marital or family status 10. Religion 11. Education 12. Financial information 13. Criminal information 14. Employment information 15. Personal views or opinions, except if they are about someone else

- If yes, go to Part 2

- If no, answer question 1.5 and submit questions 1 to 1.5 to pia@viu.ca. You do not need to complete the rest of the PIA template.

1.5. How will you reduce the risk of unintentionally collecting or disclosing personal information?

Some initiatives that do not require personal information are at risk of collecting, using, or disclosing personal information inadvertently, which could result in an information incident.

N/A

Part 2 – Collection, Use, and Disclosure

This section will help you identify the legal authority for collecting, using, and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

2.1 Four point "Necessity Test" for the collection, use, and disclosure of Personal Information.

To determine if the Personal Information from your initiative meets the necessity threshold, apply the following four-point test to each element of PI from 1.4 above. Note that each element of PI must meet all four points of the test.

Four point "necessity test" for collecting personal information (OIPC Canada, 2016).

1. The information is rationally connected and demonstrably necessary to an operating program or activity
2. The information is likely to be effective in meeting the objectives of the program or activity
3. There are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity
4. The loss of privacy is proportional to the objectives of the program or activity

Personal Information element	Does it meet all four points of the necessity threshold?	Reasons for keeping or excluding from initiative
Sensitive student and employee records	Y	VIU staff will use EFax services to transmit all kinds of records which may include sensitive personal information.

2.2 Does your initiative involve the use of Artificial Intelligence (AI)? If so, please fill out Appendix One: GenAI Analysis Questions

N/A

2.3 Personal Information Flow Diagram and/or Personal Information Flow Table

In the table below, list the personal information from question 1.4. Think about how each element of information flows through your project. Your Privacy Officer can help you figure out whether each step is a collection, use, or disclosure, and whether you have the legal authority for the way you're working with the information. Alternatively, you can attach a flow diagram to this PIA. Add rows as necessary.

	Describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**(Collection, Use or Disclosure)**	**FIPPA or other legal authority (Privacy Office)**
E.g.	*E.g., Student email, password, and IP address collected by software platform for account creation.*	*Collection*	*FIPPA 26(c) "info relates to and is necessary for a program or activity"*
1.	Authorized VIU staff member connects to OpenText client via SSO and may be prompted with MFA (VIU Security protocols)		
2.	VIU staff member sends records that contain student/employee PI to internal or external parties.	Use, Disclosure	Usually s. 33(2)(d) (used for purpose for which obtained or consistent with purpose of collection). However, each individual area should have PIA on file.

3.	Faxed records are transmitted to a secure OpenText Fax server. The recipient logs into the secure OpenText Fax server to view the fax.	Use, Disclosure	Same as previous
4.	VIU staff member receives records that contain student/employee PI from internal or external parties.	Collection	Usually s. 26(c): the information relates directly to and is necessary for a program or activity of the public body. However, each area should have PIA on file to address collection.
5.			
6.			

2.4 Risk Mitigation Table

Thinking through the information flow, identify where there are risks for privacy incidents or data breaches. For each risk, identify a mitigation strategy, as well as the likelihood of an incident, and level of impact or harm if people's information were breached.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact/harm**

1	Data intercepted during transmission (e.g., if Transport Layer Security (TLS) is not enforced, or if data is misrouted by email relays). Sensitive personal or health information could be exposed.	Ensure TLS encryption in transit (email to fax server, fax server to recipient). Conduct regular penetration and configuration testing.	Low	High (exposure of personal/health/financial records).
2	Unencrypted storage of faxes on OpenText servers creates risk of insider access or data breach.	Confirm provider uses AES-256 encryption at rest. Vendor risk assessment and security attestation (SOC 2, HIPAA, PIPEDA compliance). Limit storage retention (auto-delete faxes after X days).	Medium	High (large-scale breach could expose all transmitted data).
3	Weak or shared passwords for fax/email accounts leading to unauthorized access.	Enforce MFA on all accounts. Use least-privilege access (role-based). Quarterly access reviews and account audits.	Medium	High (could expose all received/sent faxes)
4	OpenText as a third-party vendor could suffer a breach, exposing stored/processed data.	Vendor due diligence: review SOC 2 / HIPAA compliance reports. Ensure data residency in Canada. Include breach notification SLA in contract.	Low-Medium	High (external compromise = large data set exposed).
5	End-users may download fax attachments to unsecured personal devices, or sync them to unencrypted drives/clouds.	Enforce endpoint security controls (disk encryption, anti-malware, MDM for mobile). Educate staff on secure handling and deletion (VIU Privacy & Access course). Restrict printing to managed devices.	Medium	High (localized breach, but significant if personal health or financial data involved)

2.5. Collection or Privacy Notice

If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice, also known as a privacy notification.

A collection notice must contain the following elements:

16. The legal authority and section under FIPPA under which you are collecting personal information.
17. The purpose for which you are collecting the personal information and how it will be used.
18. The contact information of an employee or officer at VIU who can answer questions about the collection of personal information.

Contact the privacy office for a collection/privacy notice template.

If applicable, paste your privacy notice here.
N/A

Part 3: Storing Personal Information

3.1. Is any personal information being stored outside of Canada?

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

All data is stored in Canada.

3.1.1. Where is the personal information stored?

3.2. Does your initiative involve sensitive personal information?

Examples of sensitive personal information include personal health information, genetic and biometric data, personal finances, geolocation data, criminal records, counselling records, HR records, payroll records, racial or ethnic origin, sexual orientation, religious, philosophical, or political beliefs, etc.

Yes

If **yes**, please complete **Part 4**: Assessment for Disclosures of Sensitive Personal Information.

If **no**, skip to **Part 5**: Security of Personal Information

Part 4: Assessment for Disclosures of Sensitive Personal Information

Complete this section if you are disclosing sensitive personal information. You may need help from your organization's Privacy Officer.

4.1. Is the sensitive personal information stored by a service provider?

Yes

If yes, fill out the table below, then go to question 4.3. If no, continue to question 5.

Information about Service Provider

Name of service provider	Name of cloud infrastructure and/or platform provider(s)	Where is the sensitive personal information stored (including backups)?
Open Text	Open Text Servers	

4.2. Provide details on the disclosure, including where and how the personal information is stored.

Answer this if question 4.1 does not apply. Be specific about where and how the information is being stored.

N/A

4.3. Is there a contract that includes privacy-related terms?

If there is a contract with the provider, please describe any privacy-related terms in the contract, or attach the privacy schedule.

Part 5: Security of Personal Information

Section 30 of FIPPA imposes a duty on the public body to prevent unauthorized access to Personal Information both internally and with any contracted third parties. As such, we need to make sure that personal information is safely secured in both physical and technical environments. **For each item in this section, please describe the security measures for both the service provider and for VIU internally.**

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

For example, physical security measures may include: the security environment of vendor's data centres; storing records containing PI in locked storage rooms, offices, and/or filing cabinets with controls over distributions of keys/access; locked workstations that do not permit others to view your screen (including when working remotely, etc.

Physical safeguard	VIU	Third Party
Restricted access to property (e.g. key card access)		
Security monitoring building		
Locked doors		
Locked filing cabinets		
Locked workstations		
Security cameras/ video surveillance systems		
Other:		

s. 15(1)(l)

5.2. Please describe the technical security measures related

E.g. Encryption standard for data in transit and data at rest; firew ed documents, etc.

Technical Security Measure	
Strong password requirement	
Multi-factor authentication (MFA)	
Role-based access	
Encryption in transit	
Encryption at rest	
Isolation control: Application	
Isolation control: Network	
Isolation control: Database	
Vulnerability scan	
Vulnerability penetration testing	
Configuration management	

Patch management	[redacted]
Technical control: perimeter firewalls	
Technical control: Web application firewalls	
Technical control: Distributed denial of service	
Technical control: Intrusion prevention systems to control traffic flow	
Other: The OpenText network and external interfaces to the system (web service APIs, etc.) were designed to provide information protection to standards defined by organizations like the Council on Cyber Security, NSA and NIST. OpenText meets or exceeds the guidelines defined by these organizations for the protection of sensitive information. To that extent, OpenText employs multiple layers of security also known as a "Defence in Depth" that provides its customers an even greater level of protection against eavesdropping or other forms of cyber-attacks.	
Other	

s. 15(1)(l)

5.3 Tracking Access / Access Controls. In this section, you will describe how the unit will minimize the risk of unauthorized access to Personal Information.

5.3.1. FIPPA section 30 requires public bodies to manage access to PI based on the principle of "need to know" – that users may only access information that is necessary to do their job. This is frequently accomplished by assigning role-based access controls (RBAC), and by establishing a security matrix that describes which positions/roles are permitted to access specific types or groups of Personal Information. Access to personal information should only be permitted to those who demonstrate their right of access on the security access chart. Please describe how access controls work in the department, or with this initiative. Describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Each department will have its own access control plan.

5.3.2 How will you know if sensitive personal information is accessed, including access by service providers? This should include a description of what information is available through logs.

For high security environments like personal health information, OpenText makes every attempt to **NOT store any fax image data/content except for the life of the actual fax transmission**. While OpenText will

maintain all call record details (eg. fax number dialled, actual connect time, remote fax system ID, pages delivered), all fax image data is immediately destroyed upon termination of the call, whether a success or failure is detected. This is an optional setting controlled by the client. EMR providers can ensure that data is only kept on OpenText servers for the minimum time possible.

During the in-transit period, all fax image data resides in a temporary data store and remains encrypted preventing even OpenText personnel from observing the contents of the fax image/content.

Once the fax transmission has terminated, all fax/image content is FIPS-140 deleted and permanently removed from the OpenText network altogether.

In the event that any data is stored in OpenText servers for any period of time, these files are AES256 bit encrypted and can only be accessed by the client upon a valid login. All connections to the OpenText portal during login are SSL encrypted.

5.4 What controls does the provider have in place to prevent unauthorized access to sensitive personal information?

Describe technical, administrative, and/or policy measures in place to protect PI. If using a cloud-based service provider, include a description of controls in each layer of the stack: software level, platform level, infrastructure level.

User Authentication: Users can access the OpenText service via Email or online only with a valid username and password combination which are SSL encrypted. An encrypted session ID cookie is used to uniquely identify each user. While logged into our servers, all communications will be encrypted at all times.

Application Security: Our robust application security model prevents any OpenText **customer from accessing another's data. This model enforced for the entire duration of a user session.**

Organizational Safeguards: The information contained in faxed documents is proprietary to the customer sending the fax. OpenText employees do not have access to the OpenText production equipment, except where necessary for system management, maintenance, monitoring, and backups. The OpenText servers that process faxes are in a secure environment that is accessed by a team of approved professional engineers and security specialists only. As a result, all information passing through OpenText server environment remains protected and secure.

Physical Safeguards: All OpenText fax production equipment is housed at a facility that provides 24-hour physical security, redundant electrical generators and other backup equipment designed to keep servers secure and continually up and running. OpenText leverages the strongest encryption products to protect customer data and communications, including 2048-bit SSL Certification and 2048 Bit RSA public keys. The

lock icon in your internet browser indicates that data is fully shielded from access while connected to our servers.

Perimeter Defense / Operating Systems: [redacted] s. 15(1)(l) [redacted]

Reliability and Backup: [redacted]

No Storage Option: Clients have the option to set their account to delete fax data once it has been delivered or retrieved. Immediate deletion of the data once it has been delivered ensures maximum protection of any private health information. All of these security features are designed to exceed HIPAA Compliance specifications.

Part 6: Accuracy/Correction/Retention of Personal Information

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

6.1 How is an individual's information updated or corrected?

FIPPA section 29 states that a person can ask you to correct their personal information in your custody or control. If it is not possible to update or correct (for physical, procedural or other reasons) it must be noted on the record. **Please explain how it will be updated or annotated. If personal information will be disclosed to others, how will VIU notify them of the update, correction, or annotation?**

N/A – information is not being stored by the service provider.

6.2. Does your initiative use personal information to make decisions that directly affect an individual? FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

N/A

6.3. Do you have a records management schedule in place?

How long will you keep the personal information collected? Is there a plan in place for retention and deletion? Please also use this question to note how long it will be stored by the service provider (if applicable).

N/A

Part 7 – Personal Information Banks

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

7.1. Will your initiative result in a personal information bank?

No

If yes, please complete the table below:

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved

Business contact title and phone number for person responsible for managing the Personal Information Bank

Part 8 – Further Information

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

No

8.2. Will the information collected be used for research or statistical purposes?

N/A

Part 9 – Summary and Proponent Responsibility

This section is for Privacy Office recommendations as well as any limitations due to privacy concerns.

Part 10: Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Reviewed by	Privacy Officer
Approved by	ITS, Web Management
Date:	2026-01-13