VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for Non-Ministry Public Bodies
Jamf Pro for Business

Table of Contents

VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for Non-Ministry Public Bodies
Jamf Pro for Business

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Jamf Pro for Business
Organization:	Vancouver Island University (VIU)
Branch or unit:	Information Technology Services (ITS)
Your name and title:	Shelly Korobanik, Privacy Consultant
Your work phone:	250-308-5457
Your email:	shelly@privacyworks.ca
Initiative Lead name and title:	Brad Moran, Business Architect
Initiative Lead phone:	250-753-3245 x4003
Initiative Lead email:	Brad.moran@viu.ca
Privacy Officer:	Bill Boyte
Privacy Officer phone:	
Privacy Officer email:	William.Boyte@viu.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No this is not a data-linking initiative.
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No this is not a common or integrated program or activity.
Related PIAs, if any:
PIA Microsoft Office 365 PIA Apple Business Manager

1. What is the initiative?

Jamf Pro for Business (hereinafter referred to as Jamf Pro) is a mobile device management (MDM) hosted solution that securely automates the tasks associated with Apple device deployment, management, and inventory to deploy devices without having to physically touch the device. Apple devices purchased by VIU will be automatically registered through Apple Business Manager (ABM) which is also being implemented.) ABM's integration with Jamf Pro automatically enrolls the iOS devices in Jamf Pro with all MDM-specified configurations, restrictions, controls, apps, etc. automatically installed. Jamf Pro is hosted in Amazon Web Services (AWS) Canadian-based datacentres.

VIU intends to use Jamf Pro for:

- Synching user accounts with VIU's public tenant of Microsoft Azure Active Directory (AAD) to enable user account management to be conducted using Jamf Pro
- Modifying configurations and settings on remote devices – for example the default iCloud storage setting will be changed from iCloud to VIU's OneDrive. Although users can manually change this setting, it is a preventative measure that was not available to VIU prior to use of Jamf Pro to mitigate the risk of VIU data being stored in users' iCloud.
- Deploying new software installs and updates remotely
- Remote control/screen sharing as part of IT support
- Remote access of file system / installed applications as part of IT support
- Zero Touch deployment (allowing pre-set configurations to happen when the initial user logs in, rather than requiring a technician to set it up)
- Remotely securing stolen/lost devices through remote locking and wiping capabilities.

Jamf Pro's integration with AAD through federated authentication will allow VIU users to log into their assigned or shared device using their AAD credentials to access a self-service app for organizationally approved apps, software, and content. [redacted] s. 15(1)(l)

As per the Software Licences and Services Agreement (SLASA - Appendix A) and associated Data Processing Agreement (DPA)[1]:

- VIU retains control over all content entered in to the Jamf Pro system;
- VIU is responsible for notifying its users and obtaining all necessary consents in accordance with FIPPA;

[1] https://www.jamf.com/resources/product-documentation/data-processing-agreement-for-jamf-customers-faqs/

- VIU as a Canadian customer will have its data hosted on Amazon Web Services (AWS) in Canadian based data centres;
- Jamf will not have access VIU data as part of any Services except as stipulated in the SLASA, and will ensure that all personnel performing support services are properly trained and supervised;
- Upon termination of Jamf Pro hosted services, Jamf will provide VIU with a copy of the most recent backup of their database if requested in writing within 20 days after the effective termination date, otherwise the data is deleted and a certificate of destruction provided.

An indemnity approval letter (Appendix B) for the ABM Agreement has been obtained from the Ministry of Finance, Risk Management Branch and Government Security Office.

This assessment was conducted to enable procurement of the Jamf Pro solution and is based upon information without availability to the application itself. Subsequently it has been noted in the risk table that if the Jamf Pro solution is procured, a review of this assessment should be conducted to ensure its accuracy and a PIA Addendum completed in the event of inaccurate and/or other significant information being discovered.

2. What is the scope of the PIA?

The scope of this PIA is for the Jamf Pro Business cloud-based MDM solution.

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

Data elements involved in this initiative are the elements synced from AAD which may include the following:

- First, middle, and last name
- Managed Apple ID

Additional fields in AAD user profiles will be synced with Jamf Pro but are not required for the service:

- Role
- Email address - note that for students their VIU email is based on their student number (studentnumber@viu.ca) but this may change to their name in future as noted in the PIA Addendum – Office 365 Updates.

3.1 Did you list personal information in question 3?

Personal information 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.

Type "yes" or "no" to indicate your response. **Yes**

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

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

There is no collection of personal information involved in this initiative, just a use of existing personal information in AAD.

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.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to 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 authority	Other legal authority
Step 1: Jamf Pro syncs to VIU's AAD	Use	s. 32(a)	

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice

There is no collection of personal information involved in this initiative, just a use of existing information when syncing Jamf Pro with VIU AAD.

PART 3: STORING PERSONAL INFORMATION

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

7. Is any personal information stored outside of Canada?

Type "yes" or "no" to indicate your response. **No**, Jamf Pro stores VIU information in AWS data centres in Canada.

8. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response. **No.**

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

Type "yes" or "no" to indicate your response. **Not applicable**

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

After you answer this question go to Part 5. **AWS servers in Canada**

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA – N/A

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

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

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

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

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

13. Does the contract you rely on include privacy-related terms?

Type "yes" or "no" to indicate your response.

- If yes, describe the contractual measures related to your initiative.

15. **What controls are in place to prevent unauthorized access to sensitive personal information?**

16. **Provide details about how you will track access to sensitive personal information.**

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases or information systems?

Type "yes" or "no" to indicate your response. **Yes**

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

Type "yes" or "no" to indicate your response. **No**

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

As per the Support Licences and Services Agreement, section 17: Information Security and Data Processing, Jmaf will "*implement and maintain appropriate administrative, physical, technical and organizational safeguards and security measures designed to protect against anticipated threats to the security, confidentiality or integrity of Customer Content. We will, at a minimum, maintain the security of Customer Content in accordance with the Jamf Information Security Schedule that is available at https://www.jamf.com/trust-center/legal." See Appendix C for Jamf Information Security Schedule.*

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	X
Employees that need standing or recurring access to personal information must be approved by executive lead	N/A
We use audit logs to see who accesses a file and when	X
Describe any additional controls:	Jamf Pro user roles[2] to restrict access: • Administrator: a privilege set granting full Create, Read, Update, and Delete privileges. • Auditor: a privilege set granting read-only access to Jamf Pro. • Custom: allows granular privilege assignments. • Enrollment Only: a privilege set granting enrollment rights in Jamf Pro and Recon. Note that custom roles will be developed when Jamf Pro is installed.

[2] https://docs.jamf.com/10.37.0/jamf-pro/documentation/Jamf_Pro_User_Accounts_and_Groups.html

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

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

Personal information is Jamf Pro is synced from VIU's AAD which is presumed to be accurate and correct as source systems managed by Human Resources (for staff) and Registration (for students) as used to create VIU's AD from which AAD is sync'd.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Type "yes" or "no" to indicate your response. **Not applicable.** No manual corrections are made directly in the Jamf Pro system. Changes to source systems would be as per existing VIU processes related to the HRIS (Human Resource Information System) or SRS (Student Record System) portals.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response. **See 22.1.** Management of source system records by Human Resources and Registration departments would be in accordance with existing VIU policies and procedures.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response. **Not applicable.** Jamf Pro is synced with AAD so any changes to information would be updated automatically.

23. Does your initiative use personal information to make decisions that directly affect an individual?

Type "yes" or "no" to indicate your response. **No.**

- If yes, go to question 25
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

Type "yes" or "no" to indicate your response. **Not applicable**

- If no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

Type "yes" or "no" to indicate your response. **No.**

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

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

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

Type "yes" or "no" to indicate your response. **Yes a PIB is created.**

- If yes, please complete the table below.

Describe the type of information in the bank
Demographic and contact information
Name of main organization involved
VIU
Any other ministries, agencies, public bodies or organizations involved
Jamf
Business contact title and phone number for person responsible for managing the PIB
Bill Boyte, General Counsel and University Secretary

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible risk	Response
Risk 1: This PIA was conducted in order to procure the Jamf Pro service without having access to the actual system. Subsequently there is a risk that details provided are not accurate which could result in unknown risks to privacy.	Personal information involved in this initiative is minimal (student ID, name and email) so level of harm from an unknown risk would be considered low. Once access to the application is available, a review of the details provided in this assessment should be conducted and any inaccuracies or missing details of significance documented in a PIA Addendum.
Risk 2: Although there is no new collection of personal information by VIU, VIU has not implemented a collection notice for all users and subsequently continues to be at risk of non-compliance with FIPPA.	VIU staff and students[3] are required to read and accept policy 45.01 Use of Information Technology as part of the onboarding process, so it is recommended that a notice of collection be incorporated into that policy as a mitigation strategy.

[3] https://isapp.viu.ca/acct_maint/stu_accounts/student_accounts.asp

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Approved subject to subsequent amendments as appropriate.

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Bill Boyte, General Counsel and University Secretary	[redacted] s. 22(1)	April 22, 2022

Program Area 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.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Brad Moran		
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate Only required if personal information is involved	Marlene Kowalski, CFO and Project Executive Sponsor		

APPENDIX A – Jamf Software Licences and Services Agreement

jamf-slasa-2021.pdf

APPENDIX B – Indemnity Approval Letter

BRITISH COLUMBIA

January 21, 2022
202213942

Marlene Kowalski
Chief Financial Officer and VP Administration
Vancouver Island University
900 5th St
Nanaimo, BC V9R5S5

Sent via email: contractservices@viu.ca

Dear Marlene Kowalski:

Re: Indemnity Approval

Pursuant to section 2(1) of the Indemnities and Guarantees Regulation, BC Reg 153/2018, as Executive Director of Risk Management Branch, of the Ministry of Finance, I approve of the proposal for the indemnity(s) in the Software License and Services Agreement between Vancouver Island University and Jamf Software, LLC with regards to support for Apple, Inc. devices. I do hereby give my written assurance that the indemnity(s) has been reviewed and accepted by the Risk Management Branch.

This approval is subject to the understanding that any payments made pursuant to the indemnity(s) would be from Vancouver Island University's own account.

[redacted] s.22(1)

Linda Irvine
Executive Director
Risk Management Branch
Ministry of Finance

LI/BJ

Attachment

Ministry of Finance | Risk Management Branch | Mailing Address: Box 9405 Stn Prov Govt Victoria BC V8W 9V1 | Telephone: 250 356-1794 Facsimile: 250-356-6222

APPENDIX C - Jamf Information Security Schedule

Information_Security
Schedule(for_trust_(

APPENDIX D - Jamf Data Processing Agreement (DPA)

Jamf-Customer-DPA.
pdf

--END--