PIA02636 — Jamf Pro Cloud

PIA REVIEW – EXECUTIVE REPORT

PREFACE

This document forms part of UBC Safety and Risk Services (SRS) PrISM's internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Christian Stockman	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2023-06-23	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-06-23	Ryan Pannell	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

UBC uses Jamf, a USA-based device management platform that enabled IT staff to manage Apple devices (owned/managed by UBC) in a centralized environment. The tool allows for central management, logging, patching tracking and other security purposes in an efficient manner. Jamf Pro is already an enterprise-wide solution that is used by both UBC IT Vancouver & Okanagan and hosted/administered by the UBC IT Okanagan Desktop Architecture Team. The University will be moving its on-premise instance of Jamf Pro to Jamf Pro Cloud to leverage economies of scale and resources at the University. Specifically, UBC will be moving from a self-hosted implementation to a cloud implementation so to eliminate the need to manage infrastructure and focus more on service delivery.

Personal information collected by the service is minimal or considered business contact, and is required for the service to be used. Review of the Jamf SOC 2Type 2 Report and associated security documentation indicates robust security practices are in place to protect personal information. Jamf is hosted on AWS, which has also been reviewed by the PIA team.

1.2 Description of the Program, System, Application, or Initiative Assessed

The purpose of this project is to migrate the University of British Columbia's (UBC) current self-hosted implementation of Jamf Pro to Jamf Pro Cloud. With Jamf Pro Cloud, UBC can use a cloud-based platform that provides greater scalability and flexibility, automatic updates, and disaster recovery capabilities. This eliminates the need for on-premises infrastructure and dedicated resources to update, patch and maintain the infrastructure.

1.3 Scope

Use of JAMF Pro Cloud by UBC IT and other support staff who are authorized to use the service.

1.4 Data Elements

Personal information has already been collected by UBC, is already on file and will be required to be collected in the context of using the service. PI is collected from Apple Device, EAD and LDAP.

Students:

- CWL Username
- Workstation login history (3 months)

Faculty/Staff:

- CWL Username
- Full Name
- Email
- Phone Number
- Position
- Department
- EAD Company
- EAD Division / Department
- Workstation Login History
- Workstation Device Information
- Workstation IP Address

1.5 Storage or Access Outside of Canada (including back-ups and recovery)

Personal information is stored on AWS data centres in the USA. UBC would use the us-west-2 hosted data region (Oregon, United States) until a Canadian data centre is available. The personal information data elements are not considered to be sensitive in the context of FIPPA legislation or UBC Information Security Standards, therefore an enhanced PIA was not completed for this initiative.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.

1.7 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

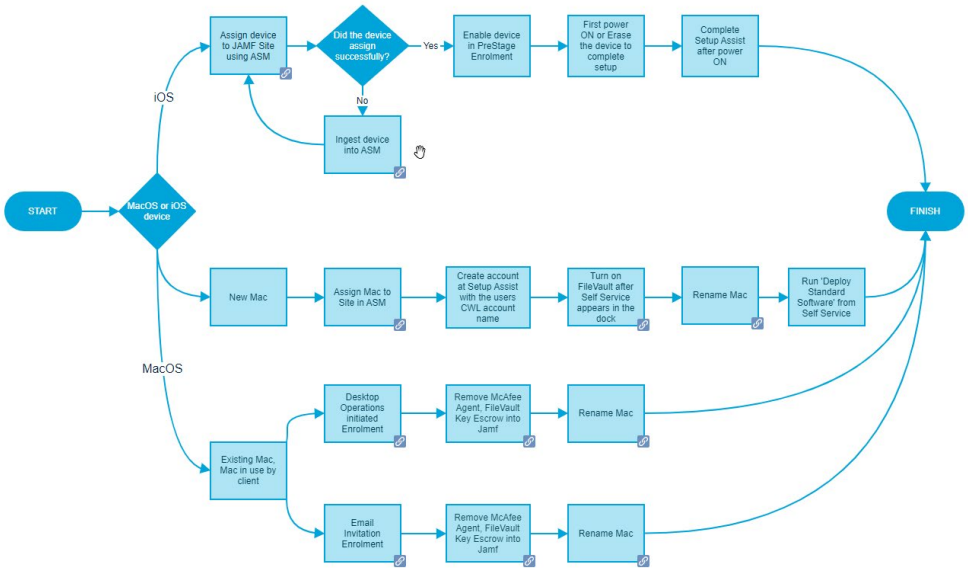
Jamf PRO, developed by Jamf and currently hosted by UBC Okanagan, is a comprehensive endpoint management solution for Apple devices, such as MacBook, iMac, MacMini and iPad.

Managed Apple devices (macOS and iOS) periodically communicate with back-end JAMF Software Server (JSS) through an encrypted communication that was configured during the device enrolment. For macOS devices, such as MacBook, iMac and MacMini, a software agent will be installed on the device in addition to Mobile Device Management Profile.

Additional information about the service is available at:

- https://it.ubc.ca/services/desktop-print-services/university-computer-management-service/ucms-apple-devices
- https://confluence.it.ubc.ca/display/itdesktop/Jamf+Pro

The following data flow diagram outlines the use of Jamf and enrolment process at UBC:



2.2 Risk Mitigation Table

The following table outlines risk identified in relation to the project and recommended response plan.

Category: Privacy					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
PI stored / accessible outside of Canada	RK0021429	4 – High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Limited personal information (primarily considered business contact) will be stored outside of Canada. This is authorized without consent under FIPPA amendments made in late 2021				
Inadequate controls for volume of personal information	RK0021525	3 - Medium	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The Jamf solution is currently in use, Move to the cloud instance will not compromise use of the service or security. The cloud service has been vetted by UBC IT Security teams, and the PIA Team has reviewed available security documentation to determine a level of comfort with transitioning to the cloud instance.				

2.3 Collection Notice

Not Required.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

Not applicable.

2.5 Consent Withheld Procedure

Not applicable.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.4 Tracking Access / Access Controls

UBC: Active Directory (AD) grants user access and users are part of AD groups. Authenticated users can only see details for the specific groups they support. Only IT staff and edge administrators can access/authenticate to the application.

Jamf: Jamf Cloud Operations staff may log in to the servers hosting Jamf Pro to access settings related to a support issue. In rare cases, Jamf Cloud Operations staff may also need to access your database to resolve a support issue. In this event, Jamf Cloud Operations staff will do their best to respect your privacy, and will only access the files and settings needed to perform the required tasks. All activity performed by Jamf employees within our cloud environment is logged and monitored. SSO, VPN, and MFA are used to dictate user access.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

This project does not capture personal information that directly affects an individual.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under s.(35) of FIPPA.

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Overall provided information was deemed reasonable to provide an understanding of operating privacy and security controls.

Information Reviewed	Date Received
Jamf Architecture Diagram.pdf	2023-05-17 22:59:35
Jamf Cloud SOC 2 Type II Report 11.19.21.pdf	2023-05-17 22:59:35
Jamf Cloud SOC2 Bridge Letter 03312022.pdf	2023-05-17 22:59:34
Jamf Information Security Policy.pdf	2023-05-17 22:59:34
jamf-cloud-next-steps.pdf	2023-05-17 22:59:35
Jamf-Customer-DPA.pdf	2023-05-17 22:59:35
Jamf-Pro-Enrollment-Process.png	2023-05-17 22:59:34
Re_ UBC Jamf Pro Cloud.pdf	2023-05-17 22:59:34

6.2 Analysis and Findings.

Based on the information provided, our review has concluded there are no significant privacy or security risks introduced by this project or use-case. The project may proceed in the proposed manner as long as it continues to fully comply with the FIPPA legislation and the UBC Information Security Standards, subject to the conditions of approval in the next section.

6.3 Conditions of Approval

None Specified.

6.4 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PrISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance
Anthony Knezevic

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To
Requestor: Justin Avdich, Client Services Manager **Project Manager:** Ryan Pannell, Support Analyst II - client services **Owner**: Anthony Knezevic, Associate Director, IT Service Delivery **Risk Advisor:** Christian Stockman, Senior Advisor, Privacy and Information Security Risk

PIA Request History:

PIA Request Date	Report Created
Anthony Knezevic	2023-05-17 16:16:42