# PIA02691 — Adobe Cloud Storage

# PART 1: GENERAL INFORMATION & OVERVIEW

## 1.1 Executive Summary

UBC has recently updated its Adobe Cloud Storage offering. Since 2018, UBC provided Adobe cloud user subscriptions with cloud storage initially disabled. However, with the renewal of UBC's Adobe licensing in July 2023, a change was introduced. Under the new agreement, UBC now includes 100 GB of cloud storage for faculty, staff, and students with active software licenses.

While this service enables users to store and share digital assets and records online, it also introduces privacy and security risks, such as data leakage, record loss, and data residency concerns. To address these risks, UBC has implemented mitigation strategies:

1. Mitigation measures include domain-specific restrictions on file sharing capabilities, with the deactivation of public links to enhance security.
2. Advising users against using this service unless necessary, requiring them to acknowledge responsibility for any associated risks.
3. Measures are in place to ensure that Adobe Cloud Storage complies with UBC's Information Security Standards, which cover aspects such as log management, administrator monitoring, and access management.

The project team is currently assessing whether the benefits of using Adobe Cloud storage outweigh the risks associated with providing all users access to this service.

## 1.2 Project Description

Since 2018, UBC has provided Adobe cloud user subscriptions, with cloud storage initially disabled. In July 2023, UBC renewed its Adobe licensing. Under the updated terms of this new agreement, UBC will now offer 100GB of cloud storage for faculty, staff, and students holding active software licenses.

Currently, the project team is evaluating whether the advantages of utilizing Adobe Cloud Storage outweigh the potential risks associated with granting all users access to this service.

### RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is 4 – **High**.
The residual risk classification level of this PIA submission at closure is 3 – **Medium**.

## 1.3 Scope

The scope of this review encompasses the privacy risks related to the use and administration of Adobe Cloud Storage at UBC. It should be noted that the mitigations detailed in this report assume that the storage feature will be enabled for all UBC individuals who are granted an Adobe license.

This review does not include an assessment of Adobe's Information Security posture. Additionally, it does not cover potential privacy risks associated with other Adobe products.

## 1.4 Data Elements

The evaluation of Adobe and Adobe Cloud Storage at UBC involves two primary categories of data elements:

1. User Account Data: This includes information collected to create Adobe user accounts. UBC provides following details to Adobe:
    a. For faculty and staff: Account creation details provided to Adobe through a partnership platform, including basic identification and contact information relevant to their location.
    b. For students: Account creation involves assigning anonymized identifiers synced from UBC's internal systems to ensure privacy while enabling service usage.
2. Digital Assets and Records: These are stored within Adobe Cloud Storage. The usage is confined to certain Adobe services. The stored digital assets are not intended to contain information classified as High Risk or Very High Risk according to UBC's Information Security Standards U1. Specific applications with the cloud storage feature enabled are detailed in Section 3.4: Tracking Access / Access Controls.

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

Adobe Cloud Storage, utilized by UBC, is hosted on Amazon Web Services (AWS) in the Virginia, USA region. Given that the data elements involved are not classified as sensitive in the context of FIPPA legislation or UBC Information Security Standards, an enhanced PIA was not deemed necessary for this initiative.

## 1.6 Data-Linking Initiative

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

## 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 FIPPA Schedule 1.

# PART 2: PROTECTION OF PERSONAL INFORMATION

## 2.1 Personal Information Flow Diagram/Table

**Faculty/Staff Adobe Account Provisioning Flow:**

1. Faculty and Staff log in to the UBC Software Download Webstore (https://ubc.onthehub.com).
2. The Kivuto webstore validates the user's affiliation and eligibility, displaying a software menu.
3. Once an order is placed, the Kivuto webstore processes it and executes license provisioning.
4. Adobe's license server subsequently assigns and activates the license.
5. Finally, the Kivuto webstore sends an order confirmation email to the user.

**Student Adobe Account Provisioning Flow:**

1. Course/Program Coordinators submit a list of courses requiring Adobe Software.
2. Student identifiers and course enrollment details are transferred to the Integrated Data Reporting team through a designated platform for processing.
3. The team compiles and uploads a spreadsheet of students' CWLs for the specified courses to a secure folder in Teamshare.
4. A random UUID is generated.
5. Adobe licenses are then assigned using the Adobe synchronization tool.

## 2.2 Risk Mitigation Table

| Privacy Risks | | | | | |
|---|---|---|---|---|---|
| **Description** | **Reference #** | **Inherent Likelihood** | **Inherent Impact** | **Response** | **Residual Risk** |
| **Inadequate information sharing controls** | RK0021524 | 4 - High | 4 - Major | Mitigate | 3 - Medium |
| | The introduction of Adobe Cloud Storage as a document storage and sharing platform for staff, faculty, and students at UBC increases the risk of data leakage. This necessitates enhanced support and monitoring by UBC IT.<br><br>**Mitigation Plan:**<br>To address the potential risks associated, the following strategies are recommended:<br>1. Domain-Restricted File Sharing: Limit file sharing to users within the ubc.ca email domain to prevent unauthorized information dissemination.<br>2. Enhanced Access Controls: Enforce protocols where users can only access documents explicitly shared with them, securing sensitive data from unintended exposure.<br>3. User Compliance and Education: Require all users—staff, faculty, and students—to be aware of and agree to these usage protocols as a condition of service access, promoting responsible document handling.<br>4. Restriction on Public Sharing: Disable the functionality for creating public links to documents, safeguarding against the accidental sharing of sensitive content with external entities.<br>These measures aim to minimize the privacy and security risks posted. | | | | |
| **Weak or Absence of Retention Controls** | RK0021677 | 3 - Medium | 4 - Major | Transfer | 3 - Medium |
| | UBC Adobe Administrators encounter challenge with limited retention capabilities in Adobe Cloud Storage, particularly when compared to similar features in Microsoft 365 products. A notable example is the 30-day recovery period for user accounts once a license is no longer assigned. This limitation poses a significant risk of record loss for students, whose access is typically limited to the duration of specific courses requiring Adobe services.<br><br>**Mitigation Plan:**<br>To mitigate these risks, the following measures are proposed:<br>1. Usage Advisory: Communicate to staff, faculty, and students the limitations of using the service for long-term storage, highlighting the retention constraints.<br>2. Retention Risk Acknowledgment: Ensure that Heads of Units (or their delegates) understand and accept the risks related to data retention. They should confirm that managing and adhering to UBC's retention schedules for records stored within Adobe Cloud Storage is their responsibility, which includes compliance with data retention policies.<br>3. Awareness of Recovery Procedures: Clearly communicate the procedures for recovering files, particularly from accounts of users who have left the institution. This includes the expectation for administrators to act within a specified timeframe to manage file recoveries.<br>Implementing these measures will help manage the risks related to the retention limitations in Adobe Cloud Storage at UBC. | | | | |
| **PI stored / accessible outside of Canada** | RK0021523 | 4 - High | 3 - Significant | Accept | 3 - Medium |
| | The use of Adobe Cloud Storage by UBC, hosted on AWS in Virginia, USA, presents specific challenges when dealing with sensitive personal information. This configuration necessitates an increased level of scrutiny and assessment, given the discrepancies in privacy data protection standards between those applicable under the FIPPA in Canada and those in the USA. The movement of data cross borders introduces notable risks concerning privacy and data security, especially in situations involving sensitive information. It is imperative to consider these jurisdictional differences as they might impact the protection and management of personal data stored or processed through this service.<br><br>**Mitigation Plan:**<br>To mitigate these risks, the following measures are proposed:<br>1. Implementation of a Privacy Notice: A privacy notice is recommended. This notice should be prominently displayed to inform users that their information will be stored outside of Canada, highlighting the potential risks and jurisdictional differences in data protection standards. This step will enhance transparency and user awareness.<br>2. Enhanced User Awareness: It is imperative that users at UBC utilizing Adobe Cloud Storage are thoroughly informed about the data storage location. They should be clearly informed about the service's usage terms, particularly the prohibition against storing Very High Risk information, as defined by UBC's Information Security Standard (ISS U1), in Adobe Cloud Storage. While explicit consent is not required, ensuring users are aware and understand these conditions is crucial for responsible use of the service. | | | | |

| Security Risks | | | | | |
|---|---|---|---|---|---|
| **Description** | **Reference #** | **Inherent Likelihood** | **Inherent Impact** | **Response** | **Residual Risk** |
| **Weak or absence of administrative security controls** | RK0021678 | 4 - High | 4 - Major | Mitigate | 3 - Medium |
| | The Adobe Cloud Storage solution at UBC necessitates the implementation of data loss prevention capabilities similar to those found in Microsoft 365 storage solutions. A key concern is that the data loss prevention features in Adobe Cloud Storage are not as robust as those in Microsoft 365. This discrepancy presents potential risks in terms of effectively safeguarding sensitive data.<br><br>**Mitigation Plan:**<br>To address this challenge, the following mitigation strategies should be implemented:<br>1. Configuration in line with UBC's ISS: Adobe Cloud Storage must be configured to comply with UBC's ISSs, ensuring a level of security parallel to the mitigation strategies defined in PIA01675 for Microsoft 365 storage solutions.<br>2. Log Management: It is essential to configure Adobe Cloud Storage logs to capture critical activities such as user logins, logouts, access to resources/files, user actions, and time stamps of modifications. These logs should be retained for at least 90 days, 365 days for ERP logs, as per ISS M8 requirements.<br>3. Administrator Monitoring: Implement adequate alerting systems or system administrators. These systems should be capable of detecting attempts to subvert data loss prevention controls, aligning with the standards set for other UBC file storage solutions.<br>4. Access Management: Implement role-based access controls, to ensure users have access only to necessary information. Regularly review and update user accounts to remove inactive or unnecessary ones. Promptly revoked access for former employees upon their departure. If feasible, disable access to the platform via mobile devices. Detailed requirements for this are outlined in ISS M2 and M3.<br><br>By implementing these mitigation strategies, UBC aims to establish compensating controls that enhance the loss prevention capabilities of Adobe Cloud Storage. This approach is designed to achieve a level of security and risk management comparable to that offered by Microsoft 365 solutions, thereby ensuring the integrity and security of data stored within the Adobe Cloud Storage system. | | | | |

## 2.3 Collection Notice

A collection notice is not required as the software will not be used to collect personal information, however its recommended users are informed that Adobe Cloud storage retains information outside of Canada.

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

No longer applicable, with the removal of data residency restrictions from FOIPPA enacted by Amendment Act (Bill 22).

## 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). It has been confirmed in prior reviews that AWS meets UBC's physical security requirements.

## 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). It has been confirmed in prior reviews that AWS meets UBC's physical security requirements.

## 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). RK0021678 outlines risk mitigation plans the project will need to adhere with to comply us UBC Information Security Standards.

## 3.4 Tracking Access/Access Controls

***License Management, Authentication, and Access***

Adobe licenses are distributed to staff, faculty, and students via their institutional accounts. Access to Adobe services is granted concurrently with license assignment. For staff and faculty, access is terminated when their institutional accounts are deactivated. Students are provided access to Adobe products only for the duration of courses that require these tools, with access revoked at the end of the course.

***Administrator Logging***

Adobe offers two types of logs for system administrators:

1. Content Logging: This log provides insights into how end users engage with corporate assets. For more details, refer to Adobe's documentation at Adobe Content Logs.
2. Audit Logging: The audit log assists in ensuring compliance, preventing inappropriate system access, and auditing unusual activities within the organization. Additional information can be found in Adobe's documentation at Adobe Audit Logs.

All logs will be retained in accordance with UBC's 90-day retention requirement, ensuring compliance with university policies.

***Adobe Cloud Storage Services***

Regarding UBC's current cloud storage solutions, most Adobe Cloud Storage features are disabled. Below is a table outlining the status of different Adobe services at UBC:

| Service Name | Enabled/Disabled |
|---|---|
| Acrobat Sign | Disabled |
| **Adobe Express** | **Enabled** |
| Adobe Portfolio | Disabled |
| Community | Disabled |
| **Device Preview** | **Enabled** |
| **Edge Inspect** | **Enabled** |
| **Fonts** | **Enabled** |
| Lightroom Web | Disabled |

| Service Name | Enabled/Disabled |
|---|---|
| Adobe PDF services | Disabled |
| PhoneGap Build | Disabled |
| **Photoshop Online** | **Enabled** |
| Publish Online | Disabled |
| Publish Services | Disabled |
| Story Plus | Disabled |
| Team Projects | Disabled |

# PART 4: ACCURACY, CORRECTION, AND RETENTION

## 4.1 Updating and Correcting Personal Information

Updating and correcting personal information in this context is not applicable. Account assignment utilizes personal information from existing UBC systems. Therefore, any updates or corrections to personal information must be made at the source.

## 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

Departments and faculties at UBC choosing to use Adobe Cloud Storage must implement and uphold appropriate records retention and disposal policies. These policies should align with individual and UBC-wide requirements. Adobe's guidelines indicate a 30-day retention period for files in the "deleted" folder. Files older than 30 days are permanently removed. Users can opt to immediately delete files from this folder.

Regarding UBC data retention and disposal upon revoking a user's Adobe license: UBC Adobe Administrators can recover records for up to 30 days post-license removal. Beyond this period, file recovery is not assured. However, Adobe Account Representatives have indicated that, upon request, Adobe Support may assist in recovering files for unlicensed users.

# 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 FIPPA s. (35).

## 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

To ensure an accurate assessment for this review, Adobe documentation was examined, and meetings with Adobe support staff were conducted. This approach was crucial in gathering all relevant information.

## 6.2 Analysis and Findings

The deactivation of Adobe Cloud Storage was considered unfeasible. Consequently, UBC has taken measures to mitigate risks. These measures include ensuring administrators have the necessary controls to comply with UBC ISSs, limiting file sharing capabilities, and advising users against using the service. Should users choose to ignore this advice, the responsibility for any resulting risks must be acknowledged by the Unit's Head (or equivalent) or their respective delegate.

## 6.3 Conditions of Approval

Conditions of Use of Adobe Cloud Storage for all Licensed Users:

**Condition #1 – Appropriate Stakeholder Approval**
Implementation for widespread use requires approval from the office of the CIO. Any final decisions must be documented in the amended PIA.

**Condition #2 – User Acknowledgment**
Users must be informed that UBC does not recommend Adobe Cloud Storage due to potential risks. They are required to acknowledge their responsibility for these risks. The acknowledgment includes:

- Acceptance of risks associated with Adobe Cloud Storage use.
- Awareness of limitations on file sharing.
- Compliance with UBC's retention requirements, recognizing that data linked to unlicensed users will be permanently deleted after 30 days.
- Understanding that Adobe Cloud Storage stores records outside of Canada and cannot contain Very High Risk data.

**Condition #3 – Implementation of Information Sharing Controls**
As outlined in RK0021524, mitigation plans should be executed to restrict users' file sharing capabilities and minimize associated risks.

**Condition #4 – Implementation of Data Loss Prevention Controls**
As specified in RK0021524, integration of Adobe Cloud Storage with UBC's existing file storage solutions is necessary for aligning data loss prevention controls.

## 6.4 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

| Assessment Acceptance |
|---|
| Anthony Knezevic |

| Distribution |
|---|
| **Requestor**: Hadi Susanto, Team Lead<br>**Project Manager**: Hadi Susanto, Team Lead<br>**Owner**: Anthony Knezevic, Associate Director, IT Service Delivery<br>**Risk Advisor**: Taylor Bohn, Information Security Risk Advisor |

| PIA Request Submission | Report Completion |
|---|---|
| 2023-05-15 | 2023-11-01 |