PIA01689 – DocuSign

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	2020-11-04	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2020-11-04	Mikhail Serebriakov	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

PREFACE **1**
Controlled Document 1
Document Control 1
CONTRIBUTORS 1
TEMPLATE REVISION HISTORY 1
TEMPLATE REVISION APPROVAL 1
TABLE OF CONTENTS **2**
TABLE OF FIGURES **4**
PART 1: GENERAL INFORMATION & OVERVIEW **5**
1.1 Executive Summary 5
1.2 Description of the Program, System, Application, or Initiative Assessed 5
1.3 Scope of PIA 5
1.4 Related PIAs 5
1.5 Elements of Information or Data 5
1.6 Storage or Access Outside of Canada (including back-ups and recovery) 6
1.7 Data-Linking Initiative 6
1.8 Is this a Common or Integrated Program or Activity? 7
PART 2: PROTECTION OF PERSONAL INFORMATION **8**
2.1 Personal Information Flow Diagram / Table 8
2.2 Risk Mitigation Table 10
2.3 Collection Notice 11
2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any) 11
2.5 Consent Withheld Procedure 11
PART 3: SECURITY OF PERSONAL INFORMATION **12**
3.1 Physical Security Measures 12
3.2 Technical Security Measures 12
3.3 Security Policies, Procedures, and Standards 12
3.4 Tracking Access / Access Controls 12
PART 4: ACCURACY, CORRECTION, AND RETENTION **13**
4.1 Updating and Correcting Personal Information 13
4.2 Decisions That Directly Affect an Individual 13
4.3 Records Retention and Disposal 13

PART 5: FURTHER INFORMATION 13

5.1 Systematic Disclosures of Personal Information 13

5.2 Access for Research or Statistical Purposes 13

5.3 Other Applicable Legislation and Regulations 13

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS 14

6.1 Information or Materials Reviewed 14

6.2 Information or Materials Not Available for Review 14

6.3 Analysis and Summary 14

6.4 Conditions of Approval 14

6.5 Review and Distribution 15

TABLE OF FIGURES

Figure 1 - Major Document Revision Approval History i
Figure 2 - Document Revision History and Revision Summary i
Figure 3 - Major Document Revision Approval History i
Figure 4 - Risk Mitigation Table 10

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

The DocuSign platform provides electronic signature technology and digital transaction management services for facilitating electronic exchanges of contracts and signed documents. With DocuSign, users can send online documents to people who need to sign them, and then collect and manage those documents. The service is designed to help organizations collect electronic signatures and manage digital transactions in a convenient and secure way.

The UBC Office of the University Counsel (OUC) has requested a review of the DocuSign platform to determine whether DocuSign meets UBC's privacy requirements and it sufficient for usability for document signing and management. The OUC wants to improve the process for signing documents using a single, secure platform, thereby reducing administrative burden. Eventually, it is envisioned that DocuSign will be implemented in other units with significant signing requirements, including eventual University-wide use.

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

This review examines DocuSign Standard, and has been requested by the OUC only. However, the findings can be broadly applied on an institutional level to enable electronic signature (e-signature) of documents, including, but not limited to, academic, administrative, financial, HR, procurement and research documents.

RISK CLASSIFICATION

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

1.3 Scope of PIA

In scope: DocuSign eSignature Standard (for desktop web and mobile app) and embedded functionality, for the purposes of completing e-signature and document management within the OUC.

Out of scope: DocuSign Business Pro; Additional and optional DocuSign features, including: ID verification add-on, workflows, identity management, bulk sending, payment collection, branding, and software integration; Personal information (PI) contained within documents sent using the DocuSign service; Enterprise-wide DocuSign functionality (requires input from additional stakeholders.

1.4 Related PIAs

This is the primary PIA for DocuSign use at UBC; see also PIA01628 and PIA01766 for related uses.

1.5 Elements of Information or Data

The service relies on a sender (the person sending the documents for signing) and the signer (the recipient of the documents and whose signature is requested).

Personal information (PI) collected: name, email address, date, signature, initial, company, title, e-signature metadata (signer's geolocation, signer's IP address, date and time the document is signed, transaction history of the envelope, image hash value, method and time of envelope deletion, sender and recipient names, email addresses, signature ID).

Device information: user IP address, geolocation, device identifiers and attributes (e.g., operating system and browser type).

DocuSign web site usage data: web log data, referring and exit pages and URLs, platform type, number of clicks, domain names, landing pages, pages and content viewed and the order of those pages, the amount of time spent on particular pages, the date and time services used, frequency of service use, error logs, and other similar information.

Cookies: third-party functional, performance and targeting cookies for analytics and marketing/promotional purposes (users may choose to opt out of most cookies).

Some of the PI collected is used to provide an audit trail, including the Envelope history, which provides a summary of the envelope and document details, and the Certificate of Completion, which includes complete details of the envelope signing events.

DocuSign also offers a mobile app. When using the DocuSign app, it may request access to the device user's camera, contacts, location, storage and possibly other device features. App users should adjust permission settings to limit access to device features and protect privacy.

Note: DocuSign Envelopes may hold documents containing a variety of PI elements about the recipient or other individuals. This review is limited to PI collected by the DocuSign platform only and does not include PI collected and stored within the contents of DocuSign Envelopes.

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

The instance of DocuSign used by UBC is hosted within Canada. UBC will not use any other DocuSign services which would disclose personal information outside of Canada. All DocuSign data (including backup data) is stored on secure servers inside Canada on Microsoft Azure servers in Toronto and Quebec City. Temporary access for repairs or troubleshooting may be performed outside of Canada and is permitted under FIPPA sec. 33.1(p).

1.7 Data-Linking Initiative

In FIPPA, "data linking" and "data-linking initiative" are strictly defined; if a project is a data linking initiative, it must comply with specific requirements under the Act related to data-linking initiative.	
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**
This is not a data linking initiative as contemplated by FIPPA sec. 36(1). DocuSign is able to link with popular third-party software suites in use at UBC, such as Microsoft Office 365, Salesforce, Workday, and others. Personal information may be shared as a result of any integration. All integrations are subject to a PIA.	

1.8 Is this a Common or Integrated Program or Activity?

In FIPPA, "data linking" and "data-linking initiative" are strictly defined; if a project is a data linking initiative, it must comply with specific requirements under the Act related to data-linking initiative.	
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**
Not applicable.	

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

To use the service UBC staff (sender) logs into DocuSign and uploads documents into an encrypted electronic envelope for delivery to the recipient (signer). Documents most often contain PI about the signer. DocuSign has no access to the contents of encrypted envelopes. Envelope links are sent to the recipient using the on premise UBC servers without additional third-party processing.

Inside the DocuSign ecosystem, the sender indicates the action required for the document (e.g. review, sign, etc.). The staff member emails the signer (either through the DocuSign system or their UBC email account) which includes a link to the document. The sender may also notify the signer via mobile text message (this option is not preferred as it uses a third-party service provider hosted outside of Canada).

When the signer is notified about a document awaiting their action, they will have the opportunity to create a personal DocuSign account. Signers who create a personal account can save their preferred signature (optional) for future use and keep track of all documents they have signed or created in DocuSign. Creating an account is voluntary, free, and not necessary to use the platform or to sign documents. If the signer chooses to create a personal account, he/she will enter into a Limited License Agreement with DocuSign.

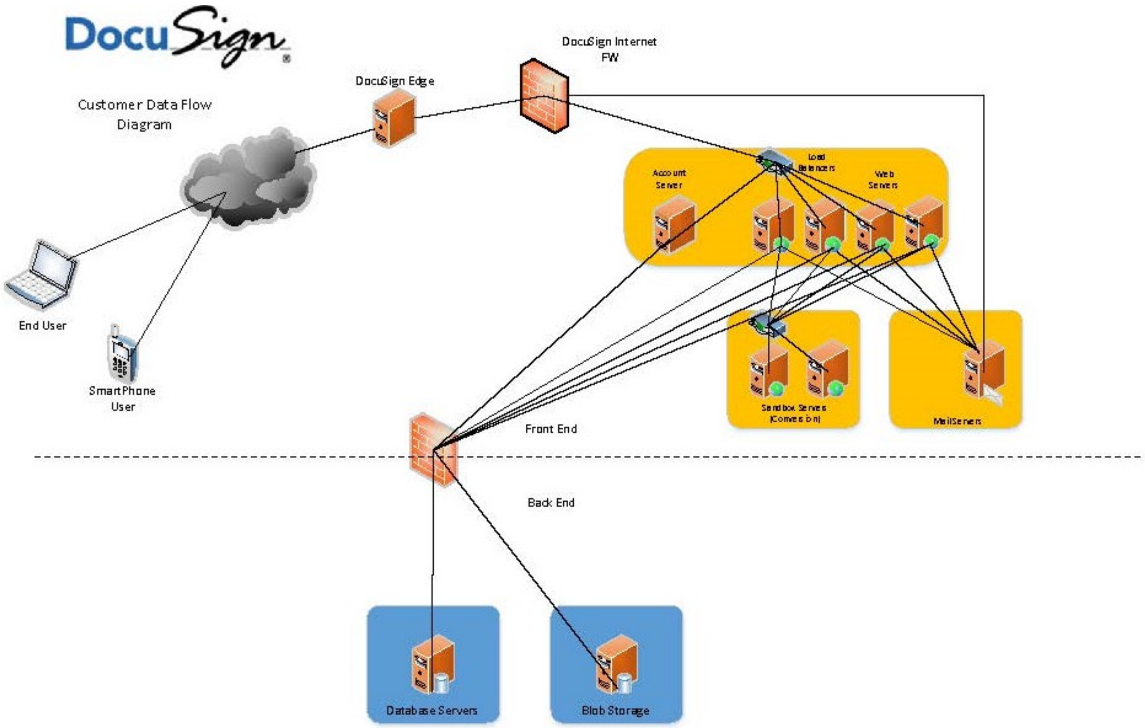
Clicking the link takes the signer to the DocuSign site where the document is waiting for their action. The document may be reviewed, printed, downloaded and comments and signatures can be added. Prior to signing, DocuSign requires the signer to read the DocuSign Electronic Record and Signature Disclosure and check the box to show that they agree to use the electronic records and signatures. This is a requirement under U.S. law but does not apply in Canada.

Signatures are encrypted and hashed to secure the signed documents and reveal whether the document has been tampered with or compromised. DocuSign generates personal information (PI) about a signer when they access and sign documents. This PI (transactional metadata) is used to authenticate the signer's signature and is maintained to establish a digital audit trail. The process results in the generation of two virtual documents, the Envelope History and Certificate of Completion. The certificate is the official 'proof' that a document has been electronically signed, and includes eSignature metadata details. These resources are associated with the signer's envelope and contain further document details providing a full audit trail of the DocuSign transaction.

Once the document is signed, the sender is automatically notified and can retrieve the electronically signed documents, the Certificate of Completion, and the uploaded government-issued identify documents (if this feature is enabled). Signers are able to obtain only copies of the signed documents, and are not granted access to the Certificate of Completion or copies of their uploaded identity documents.

The sender can monitor documents that require action and send follow up notifications to the signer. The signature process is completed by clicking the finish button, and the document is stored in the DocuSign platform, where it can be retrieved by UBC staff. Documents are stored inside DocuSign until they are removed by the sender. The sender can set retention periods for all documents uploaded into the DocuSign platform.

DocuSign Data Flow (as presented in Security and Trust Assurance Packet 2020)



2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Category: Privacy					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Not performing PIA on new system or project	RK0020269	4 - High	3 - Significant	Mitigate	2 - Low
	Mitigation Plan: DocuSign Standard can not be integrated with other applications/platforms in use at UBC. A supplementary PIA will be required for any change in use or integrations with other University systems.				
Over collection of personal information	RK0020218	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Users will be encouraged to supply only their name and email at registration, no other PI. Consent will be obtained for personal information collected at registration.				
Retaining PI longer than necessary	RK0020268	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: UBC will ensure documents are set to be removed from DocuSign after a specified time period to avoid indefinite document retention. DocuSign will retain Certificates of Completion indefinitely.				
PI stored / accessible outside of Canada	RK0020231	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The instance of DocuSign used by UBC is hosted within Canada. UBC will not use any DocuSign services that disclose personal information outside of Canada.				
Potential PI Exposure - Incomplete PIA Review	RK0020276	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Other versions of DocuSign (e.g. Business Pro) are not endorsed as many of the features have not been reviewed as part of the PIA process. A supplementary PIA will be required for any change/expansion in use.				
Inadequate governance for personal information protection including policies and accountability	RK0020287	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: UBC must ensure that users are made aware of default DocuSign settings and determine user access requirements to limit potential PI exposure. Creation of guidelines for the user community is highly recommended.				
Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Inadequate controls to safeguard mobile devices or removable media	RK0020372	3 - Medium	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: DocuSign is available for use on mobile devices and will collect PI from these devices. This PIA has not reviewed security risks associated with using DocuSign on a mobile device. Mobile devices using DocuSign must adhere to UBC Information Security Standards and Policy SC14.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

UBC collects, uses, discloses and retains personal information in compliance with the BC Freedom of Information and Protection of Privacy Act (FIPPA).

UBC uses DocuSign, a digital transaction management system that facilitates electronic exchanges of signed documents. Your personal information (PI) is collected and will be used to sign documents, execute agreements and validate your signature in the DocuSign platform, and for purposes consistent with these uses. The collection of this personal information is permitted under FIPPA sec. 26(c) and 26(d).

Using DocuSign is voluntary. It is recommended that you review the DocuSign Terms and Conditions and Privacy Policy. If you do not wish to use DocuSign, please call or email <UBC contact name, title, unit, telephone and email here> to make alternate arrangements to sign your documents.

Note: additional content may be required for some units, pursuant to their specific use-case.

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

Project is required to comply with UBC Information Security Policy (SC-14).

DocuSign is hosted on Microsoft Azure servers located in Toronto, Canada. UBC does not have direct visibility into the physical security of Microsoft Azure data centers that host the DocuSign application. UBC has relied on publicly available documentation and vendor supplied documentation to establish a level of comfort over the physical security of Microsoft Azure data centers. This review relied on a SOC 2 Type 2 report provided by Microsoft under a separate NDA in August 2019.

Physical security measures of the senders or signer's environment and computer are not within scope of this assessment.

3.2 Technical Security Measures

Project is required to comply with UBC Information Security Policy (SC-14).

The technical security measures for this initiative are fully addressed in the DocuSign Security and Trust Assurance Packet 2019/2020. The assertions in this document are supported by independent audits and certifications including ISO 27001:2013, SSAE 18, SOC 1 Type 2, SOC 2 Type 2, and xDTM Version 1.0.

Data is transferred using AES256 encryption using transport layer security (TLS).

3.3 Security Policies, Procedures, and Standards

Project is required to comply with UBC Information Security Policy (SC-14).

Based on information from earlier SOC 2 Type 2 (and reports obtained for other initiatives) and published information, DocuSign and Microsoft Azure security policies, standards, and practices are considered robust, meeting and frequently exceeding UBC security requirements.

3.4 Tracking Access / Access Controls

Beyond the use of strong passwords, DocuSign provides advanced authentication tools to validate the identity of all transacting parties. These include: SAML Single Sign On (SSO), SMS code to an alternate device, answering secret knowledge questions and voice authorization.

All customer data is encrypted and inaccessible by DocuSign staff with the exception of the system metadata that includes some PI. UBC provides anti-virus, performs regular patching on endpoints, scans all network and email traffic for malicious code and URLs, and provides disk encryption for many systems.

DocuSign provides an administrative console that includes auditing functions. This would be the primary tool for defining which accounts have access. All access to cloud services is also monitored and logs are stored for one year.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Anyone is able to create an account with DocuSign and update their personal information in that account. The envelope sender has the ability to update the recipient's personal information (as it pertains to that document only). Once signed, this information cannot be updated. Recipients also have the ability to edit tags assigned to them in the workflow unless data fields are locked. The envelope sender can also request the signer check and update their personal information (the administrator will not necessarily be notified of any changes that occur).

4.2 Decisions That Directly Affect an Individual

Use of DocuSign may contribute to decisions affecting an individual (e.g. signed offer of employment letters, dissertation reviews, and contracts). DocuSign provides eSignature services for these purposes. Usage of DocuSign does not inhibit FIPPA sec.31, which mandates such information be retained for a minimum of one year. Any such documents must be retained independent of DocuSign usage.

4.3 Records Retention and Disposal

Envelope senders determine retention policies for their documents. Envelopes containing PI processed within the DocuSign platform will remain indefinitely until removed by the user. DocuSign encourages users to set a specific retention period for all documents. At the end of this period, all documents and data would be automatically removed near-simultaneously from all locations. DocuSign retains PI contained within Certificates of Completion indefinitely, with no option of removal by the sender or the signer.

DocuSign should not be used as a repository for UBC documents/records or used for permanent storage of the document. Accordingly, DocuSign is not considered to be part of, or to create, a Personal Information Bank under FIPPA sec. 69. Notwithstanding DocuSign's records retention policies, all UBC documents processed in the DocuSign platform are required to abide by UBC records retention policies.

It is recommended that UBC request DocuSign enable a defined retention period for the University, rather than allowing indefinite retention.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

The initiative does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

There are no other applicable legislation or regulations for this review or for this initiative.

5.3 Other Applicable Legislation and Regulations

No other applicable legislation or regulations for this review or for this initiative. The legality of electronic signatures in BC was established by the Electronic Transactions Act (SBC 2001, Chapter 10) and within Canada by PIPEDA, the Personal Information Protection and Electronic Documents Act (S.C. 2000, c).

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

DocuSign: Master Services Agreement, Privacy Policy, Sites & Services Terms and Conditions, Subprocessor List, Cookie Notice, Data Residency, eSignature Subprocessor List, Trust Center BCR-P Privacy Code, Data Management and Privacy Practices for eSignature, Security Brief, Security and Trust Assurance Packet 2019/2020 (includes ICO certification and SOC2 attestation).

Microsoft: Azure SOC 2 Type 2 Report (reviewed August 2019).

Note: All DocuSign documents are applicable to desktop and mobile versions of the software.

6.2 Information or Materials Not Available for Review

Not applicable.

6.3 Analysis and Summary

The information provided for the review has established that DocuSign can be used in the proposed manner in compliance with FIPPA and UBC's Information Security Standards.

The following are the key factors in that determination:

- Personal information is collected, used, and disclosed in accordance with FIPPA;
- Personal information is collected, stored, and accessed within Canada;
- Personal information is not disclosed to third parties;
- Access to DocuSign requires use of a valid login credentials with appropriate access authorities;
- Information is kept secure during transmission and at rest.

Accordingly, DocuSign can be used as proposed subject to the Conditions of Approval. In addition, it is recommended that the relevant UBC units issue campus-wide guidelines for DocuSign use (i.e. CTLT, IT, OUC, Privacy Matters).

6.4 Conditions of Approval

Submission of supplementary PIA request is required for:

- Change to DocuSign use or service offerings (e.g. payment processing);
- Addition of ID verification feature to any DocuSign service;
- Integration with other software (e.g. Workday);
- Implementation of DocuSign Business Pro (or equivalent).

6.5 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
Paul Hancock

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

Distributed To
Requestor: Kai Syh-Yuh Hsieh **Project Manager:** Mikhail Serebriakov **Owner:** Paul Hancock **Risk Advisor:** Christian Stockman

PIA Request History:

PIA Request Date	Report Created
2020-06-29 16:36:12	2020-11-04 21:33:31