PIA01680 – Eventus

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	2020-11-02	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2020-11-02	Irene Chou	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

Eventus Virtual Fair is a platform that permits careers fairs to take place virtually. The software is produced by Whitestone Technologies, based out of Austin, Texas, USA. SFU Career and Volunteer Services is purchasing the platform, on behalf of SFU, UBC and UVIC, from Whitestone in order to organize an online virtual career and graduate and professional program fair in Fall 2020. Eventus will allow students from all three universities and alumni to interact virtually with employers and recruiters and to be connected with employment and educational opportunities. SFU Career and Volunteer Services, UBC Centre for Student Involvement & Careers, and UVIC Cooperative Education Program and Career Services organizes annual career fairs as in-person events in the past, but due to the need of social distancing during the current pandemic, this virtual platform will allow students, alumni, and employers to interact safely.

This PIA was completed as a collaborative effort by privacy officers representing SFU, UBC and UVIC, because the Universities have agreed to a hosting partnership during the 2020 global coronavirus pandemic, which has limited opportunities to in-person events.

NOTE: OFFICIAL FINAL REPORT (SHARED BY THREE UNIVERSITIES) ATTACHED TO PIA FILES IN SERVICE NOW.

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

The objective of this joint virtual fair is to bring employers and students from UBC/SFU/UVIC together. This virtual fair is an opportunity for students to network with employers and learn about the jobs employers are actively recruiting for. On average, approximately 2000 students per institution have attended our own individual fairs so we anticipate approximately 6000+ students to attend this virtual fair. However, it is open to all students from all three institutions which would be almost 100,000 students that this event is open to.

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 **2 – Low.**

1.2 Scope of PIA

The scope of this PIA is the implementation of Eventus for direct use by faculty, staff, students, and other individuals who are authorized to use these products and services on behalf of SFU, UBC and UVIC.

In scope: Use of Eventus by SFU Career and Volunteer Services in order to host a Career Services fair in Fall 2020.

Out of Scope: Use of Eventus by other departments on campus, or use of Eventus by Career and Volunteer Services for other events.

1.3 Related PIAs

This PIA document will be used collaboratively by SFU, UBC and UVIC.

1.4 Elements of Information or Data

STUDENT DATA ELEMENTS

- Name
- Email address
- Phone number
- IP address
- Device identifier
- Technical information (e.g. browser type)
- Usage data (how user progressed through site, when the user left site)
- Demographic information
- Geolocation information
- Educational information (e.g. major, graduation year, transcript)
- Work experience (resume)

POTENTIAL EMPLOYER DATA ELEMENTS

- Name
- Business contact information
- IP address
- Device identifier
- Technical information (e.g. browser type)
- Usage data (how user progressed through site, when user left site)
- Information about the internships/jobs being offered

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

Eventus data is hosted on Amazon Web Services (AWS) servers located in Toronto, Ontario.

Backups of data from the Canadian-based servers are also stored in storage servers in Canada provided by AWS. The Eventus staff is based in Austin, Texas. The AWS server maintenance teams are based in the respective location of the Canadian data centers. Eventus staff in Austin, Texas provide troubleshooting and maintenance for the Eventus software. FIPPA s. 33.1(1)(p) is the authority for access for this limited purpose.

Daily.co will provide video chat and text chat capabilities for the pre-booked video chat sessions on the virtual career fair platform. No personal information is disclosed by Eventus to Daily.co. Daily.co does not store any video, audio, or screen-sharing data from any calls. Additionally, all video calls powered by Daily.co are established with 256-bit TLS encryption. Users can download a text file of their chat when they are in the current instance of their video chat room. After a session ends, the chat is programmatically reset. The University can also programmatically delete the chat data after a video session. For further reading on Daily.co's security protocols (https://www.daily.co/security).

1.6 Data-Linking Initiative

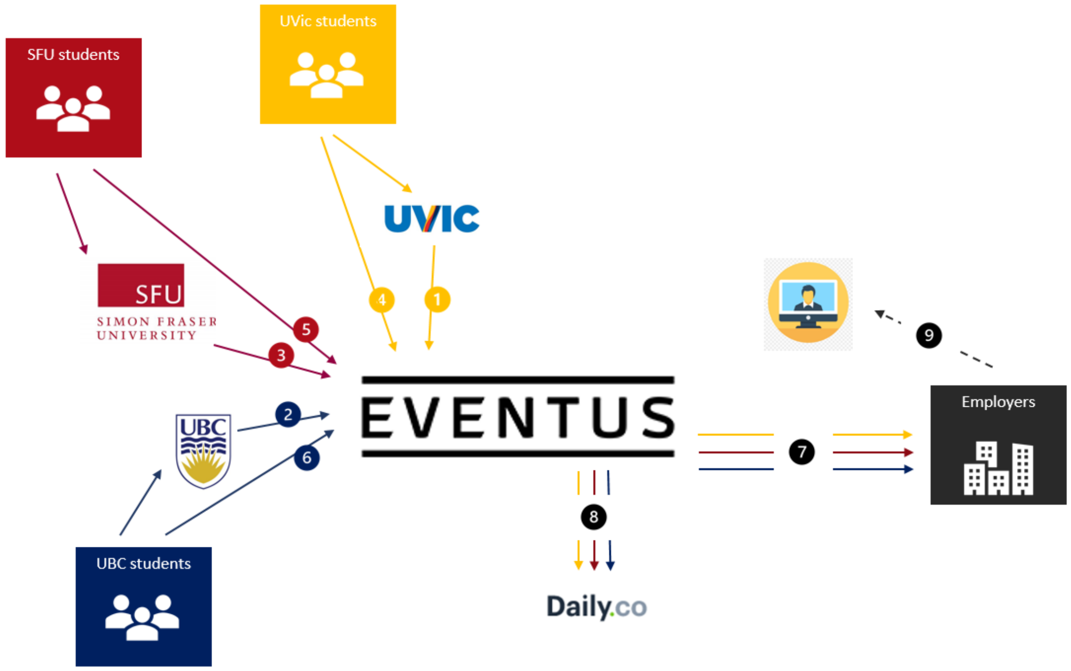
In FIPPA, "data linking" and "data-linking initiative" are strictly defined; if a project is a data linking initiative, it must comply with specific requirements under the Act related to data-linking initiative	
1. Personal information from one database is linked or combined with personal information 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.	

1.7 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



	Data Flow	Data elements	Authorization
1,2,3	UVic/UBC/SFU disclose Student PI to Eventus	Affiliation with UVic/UBC/SFU, by implication	Disclosure – 33.2 (c)
4,5,6	Eventus collects PI from UVic/UBC/SFU students	Resume; name, email	Collection – 26 (c)
7	Eventus discloses student PI to employers	Name, email, Resume (optional)	Disclosure – 33.2 (a)
8	Eventus discloses contents of video to Daily.co	Any personal information disclosed by student in meeting	Disclosure – 33.1 (p.1)
9	Employers present using their chosen video platform	Employer personal information, questions by students	Not subject to FIPPA

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**
Inadequate third-party information sharing controls	RK0020100	4 – High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: None of the parties will be data matching – Eventus will be prohibited from doing so by contract.				
Use of PI for alternate purpose	RK0020361	4 - High	3 - Significant	Mitigate	2 - Low
	Mitigation Plan: None of the parties will be collecting more PI than set out above; collection of PI by employers is outside of the scope of the PIA and not subject to FIPPA.				
PI stored / accessible outside of Canada	RK0020102	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Accessing data from outside of Canada is confined to maintenance and troubleshooting purposes by a Privacy Protection Schedule appended to the service agreement				
Inadequate controls for volume of personal information	RRK0020101	4 – High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Daily.co does not store any PI; Eventus will delete after six months in accordance with contract.				
Disclosing to or allowing unauthorized users access	RK0020360	4 – High	4 – Major	Mitigate	2 - Low
	Mitigation Plan: Eventus and Daily.co are deleting all PI / not storing any PI and are restricted by contract from subsequent disclosure.				
Retaining PI longer than necessary	RK0020362	4 – High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: Eventus and Daily.co are deleting all PI / not storing any PI				
Over collection of personal information	RRK0020359	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: None of the parties will be collecting more PI than set out above; collection of PI by employers is outside of the scope of the PIA and not subject to FIPPA.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Your personal information is being collected by UVic, UBC, or SFU for the purpose of enabling you to share that information with prospective employers. You control how much personal information you disclose for that purpose and to whom it is disclosed. This personal information is collected pursuant to s. 26 (c) of the Freedom of Information and Protection of Privacy Act. If you have any questions about the management of this personal information, please contact the following according to your university:

UVic students: privacyinfo@uvic.ca

SFU students: botelho@sfu.ca

UBC students: abraham.asrat@ubc.ca

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

The EVENTUS application is hosted on external cloud-based commercial infrastructure sites. EVENTUS is hosted at data centers within Canada owned and managed by Amazon Web Services (AWS) and Digital Ocean (Equinix). AWS is used for data storage, to store application data and backups. Digital Ocean serves as the application server in which the application's endpoints are hosted.

Physical protection of these data centers is managed by the hosting services and is reported in their SOC audits and in other security reports and reviews. The Universities rely on documentation made publicly available by Amazon and Equinix made available by EVENTUS. In addition, UBC privacy staff reviewed the Amazon data center environment in August 2019 under a separate non-disclosure agreement. The physical security capabilities of the AWS data centers meet or exceed UBC standards.

Physical security measures of each University’s faculty and staff environments and computers are not within scope of this review...

3.2 Technical Security Measures

The Universities have information security standards and policies that set out the minimum requirements for the protection of sensitive data:
Staff using EVENTUS will be expected to read, understand and adhere to the security policies, procedures and standards applicable to their University:

SFU: Fair Use of Information and Communications Technology Policy (GP24)
UBC: Information Systems Policy (SC14), Information Security Standards
UVic: Acceptable Use of Electronic information Systems (IM7200), Information Security Policy (IM7800)
In its Privacy Policy, EVENTUS states, “we use industry standard technical, administrative and physical controls to protect your data, including encrypting it at rest and as it is transferred from you to Eventus.” All data processed with the EVENTUS platform is encrypted in transmission using TLS 1.2 or above. All data is encrypted at rest using AES-128 or above.

Sub-processors

EVENTUS uses certain sub-processors to support delivery of its services. A sub-processor is a third-party data processor engaged by EVENTUS, who has or potentially may have access to or process customer data. Prior to engaging any third-party sub-processor, EVENTUS has evaluated their physical and security standards and determined that they meet industry standards for security, recoverability, and confidentiality).

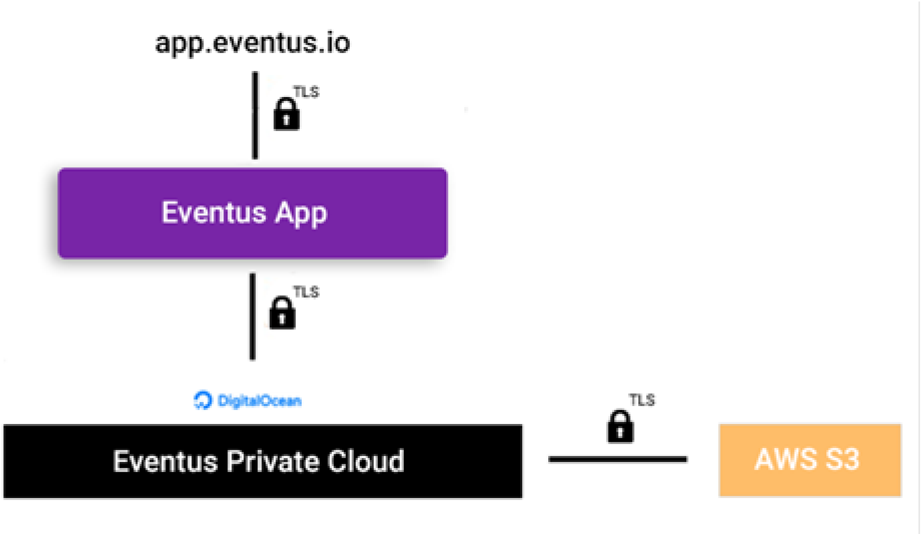
Sub-processor Identity	Sub-processing Activities	Location
Amazon Web Services	Cloud Service Provider (application data storage and backup)	Canada
Digital Ocean (Equinix)	Cloud Service Provider (application endpoint server)	Canada
Daily.co	Videoconference Capability (including Chat)	United States

EVENTUS has presented additional documentation regarding technical security information for this initiative. The assertions in these documents are supported by independent audits and certifications for the hosting services:

- Digital Ocean (Equinix): ISO 27001:2013, SOC 1 Type 2, SOC 2 Type 2;
- Amazon Web Services: ISO 27001:2013, SOC 2 Type 2, SOC 3

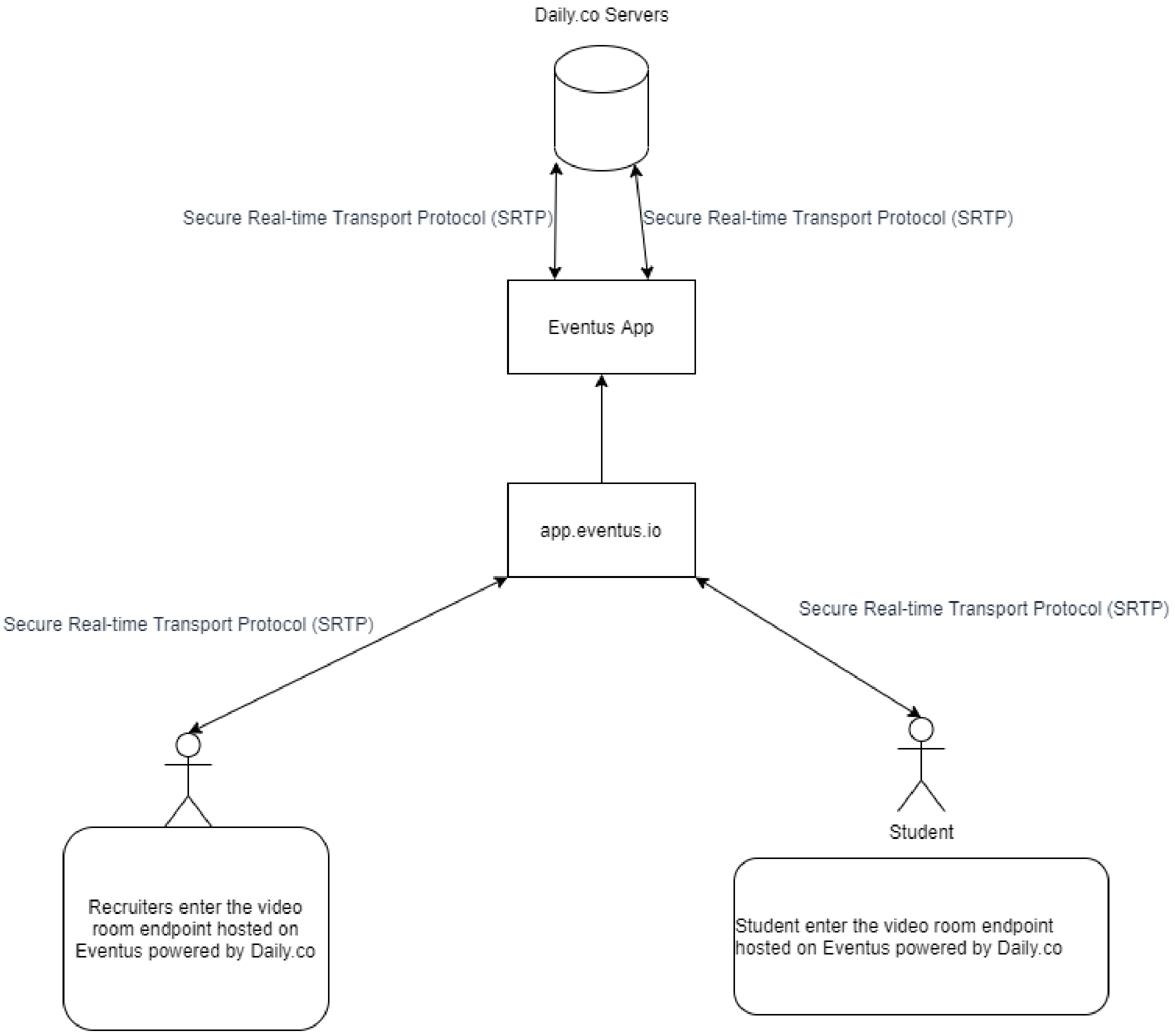
Per the SOC 2 report from Equinix, “complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.”

The sub-processor relationship for the cloud service provider component is outlined in the following diagram:



EVENTUS has not provided audit and certification information for the DAILY.CO video-conferencing sub-processing service. A review of the DAILY.CO’s publicly available Terms of Service, Privacy Policy, and Security web pages, as well as written responses from EVENTUS, indicate that all video calls powered by DAILY.CO are established with AES-256 encryption using TLS.

The sub-processor relationship for the video conference component is outlined in the following diagram:


Daily.co Servers
Secure Real-time Transport Protocol (SRTP)
Secure Real-time Transport Protocol (SRTP)
Eventus App
app.eventus.io
Secure Real-time Transport Protocol (SRTP)
Secure Real-time Transport Protocol (SRTP)
Student
Recruiters enter the video room endpoint hosted on Eventus powered by Daily.co
Student enter the video room endpoint hosted on Eventus powered by Daily.co

Details about the information collected, accessed, and stored by DAILY.CO are covered elsewhere in this PIA.

3.3 Security Policies, Procedures, and Standards

The Universities' privacy staff have had limited visibility into or access to EVENTUS' own information security policies, practices, or standards. However, EVENTUS has responded to UBC's Vendor Requirements & Risk Assessment Questionnaire (used when no third-party audit certification is present). EVENTUS has confirmed that the responses in this document are applicable to all three institutions and all data from SFU, UVic and UBC attendees.

These responses, in addition to publicly available documentation, assert EVENTUS employs robust standards and practices; however, these assertions could not be substantiated, as EVENTUS has not completed a third-party audit certification.

Based on information included in the security documentation presented as well as published information, the security policies, standards, and practices for Amazon Web Services and Digital Ocean are considered robust, meeting and frequently exceeding SFU, UBC and UVic security requirements.

3.4 Tracking Access / Access Controls

The following section describe any controls and/or ways in which the initiative will limit or restrict access or unauthorized changes.

Attendees will receive the EVENTUS event link from their institution and will need to create an EVENTUS account to attend the fair. Attendees will login to a dedicated student-facing web page offered by each University using their campus-wide login credentials. The web page will contain a link to register with EVENTUS for the virtual job fair. Thereafter, students are able to log in to the virtual career fair using their EVENTUS credentials only.

EVENTUS will segregate attendees' personal information (by University). EVENTUS technical support staff will have access to attendee personal information as required for troubleshooting purposes. University administrative staff will have access to an administrative console for the virtual job fair, but will not be able to access or view attendees' personal information. Staff will be required to register with EVENTUS for this access.

DAILY.CO does not monitor, view, or track the video or audio content or screen sharing content of meetings. Chat transcripts may be downloaded, however.

The Universities provide 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.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Typically, responsibility and accountability for processes that allow individuals to update and correct their personal information stored within University files that are used via or reside on cloud service providers are the responsibility of the University and the individual projects and initiatives which collect and process such information.

The Eventus platform requires individuals to provide personal information. Any information that an attendee provides is not accessible by University staff, and much be updates and maintained by the individual.

4.2 Decisions That Directly Affect an Individual

The use of EVENTUS in and of itself does not contribute to decisions that directly affect an individual as contemplated in FIPPA Section 31(b).

4.3 Records Retention and Disposal

EVENTUS generally retains usage data for up to six months for clients to access. After six months, EVENTUS deletes the data from their servers unless otherwise specified in the service agreement. General usage reports (not containing PI) will be retained indefinitely.

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

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

5.4 Other

This initiative is not considered to be part of, or to create, a Personal Information Bank as contemplated in FIPPA Section 69.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

The following documents available from EVENTUS were reviewed in the course of this PIA to determine underlying privacy and security issues:

- EVENTUS Virtual Fair Privacy Policy
- EVENTUS Virtual Fair Terms of Service
- EVENTUS Master Service Agreement
- EVENTUS Sub-processor List
- EVENTUS Draft Memorandum of Understanding for Joint Virtual Fair
- UBC Vendor Requirements & Risk Assessment Questionnaire (used when no third-party audit certification is present).
- Responses to University Privacy Officer Questions (August 25, 2020)
- Responses to University Privacy Officer Questions (September 20, 2020)
- Vendor Correspondence
- Meetings with Vendors and Project Representatives.

6.2 Information or Materials Not Available for Review

The following materials could not be reviewed in the course of this PIA:

- Detailed personal information data flow diagrams and tables
- Information security compliance and attestation reports, such as SOC 2 Type 2 or ISO 27001.

6.3 Analysis and Summary

The information provided for the review has established that the EVENTUS virtual career fair service can be used in the proposed manner in compliance with FIPPA and SFU, UBC and UVic policies.

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 (e.g. shared between EVENTUS and DAILY.CO)
- Access to EVENTUS requires use of a valid campus-wide login credentials with appropriate access authorities
- Information is kept secure during transmission and at rest

Accordingly, EVENTUS can be used as proposed subject to the conditions set out in the next section).

6.4 Conditions of Approval

Condition #1: Change in Use
Should the scope of the program change, further assessments may be required as new related or expanded services are considered, and through post-implementation to ensure the programs delivered match those proposed. Any contemplated changes to or use of this software that differs from the description provided in this PIA (e.g., in the collection, use, disclosure or storage of personal information) must be reviewed by the Universities for compliance with FIPPA. Consultation is also required prior to implementing any proposed changes to the implementation or use of EVENTUS.

Condition #2: On-boarding/Off-boarding
The University’s Eventus project team should develop on-boarding and off-boarding procedures to ensure only authorized staff can access Eventus.

Condition #3: Daily.co
The University programmatically delete the chat data after a video session on Daily.co.)

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
Irene Chou

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

Distributed To
Requestor: Irene Chou **Project Manager:** Irene Chou **Owner:** Abraham Asrat **Risk Advisor:** Christian Stockman

PIA Request History:

PIA Request Date	Report Created
2020-06-24 14:25:37	2020-11-02 11:27:29