PIA01659 – PODIO

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
Pimkae Saisamorn	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	Markus Fengler	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2020-11-02	Pimkae Saisamorn	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 Machine Shop is implementing an online Job Submission Form on PODIO Workflow System. PODIO, a web-based platform, allows UBC students, faculty and staff to submit jobs for production by Machine Shop staff. The form is embedded on Machine Shop website. Personal information including name, email, phone number, speed chart, job images, job deadline, drawings supplied, solid mold supplied and material available is collected as part of the job submission. A job submitter can provide an alias for first and last name and an undescriptive email address. The information will be accessed by Machine Shop staff and Shop supervisor for job production and by Administrative Staff for accounting purpose. PODIO by Citrix stores UBC data at Amazon Web Services (AWS) in Dublin, Ireland. PODIO is not integration with CWL.

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

A web-based system that allows students, faculty and staff to submit jobs for production by Machine Shop staff. Users are given links to an online submission form or an embedded form on our website. hxxp://technicalservices.mech.ubc.ca/machine-shop/support-machining-services/job-submission-form/ The system is also used to communicate with our customers (students/faculty/staff) by use of a commenting tool, chat and email features that are built into the system.

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 of PIA

The scope of this PIA is the implementation of PODIO for direct use by UBC faculty, staff and students who are authorized to use the product on behalf of UBC.

1.4 Related PIAs

Not applicable.

1.5 Elements of Information or Data

Personal information including name, email, phone number, speed chart, job images, job deadline, drawings supplied, solid mold supplied and material available is collected as part of the job submission. A job submitter can provide an alias for First and Last Name and an undescriptive email address.

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

PODIO hosts UBC data at AWS Dublin, Ireland.

1.7 Data-Linking Initiative

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

1.8 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

Not applicable.

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**
PI stored / accessible outside of Canada	RK0020074	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to implement the suggested privacy notification and consent notification at the information collection point/page before a job submitter provides personal information and submit a job.				
Retaining PI longer than necessary	RK0020195	4 - High	3 - Significant	Mitigate	2 - Low
	Mitigation Plan: The project to consult with the UBC Records Management Office (RMO) to obtain retention guideline to comply with the UBC Records Management Policy. During the course of review, we noted that the project has been advised on the records retention requirement of one year from the RMO.				
Over collection of personal information	RK0020193	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to collect only minimum personal information to fulfil the program and agree to remove phone number and job images out of the job submission form.				
Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020194	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to work with UBC IT to update the SSL certificate for Machine Shop website where hosting "Job Submission Form" to ensure it's valid and secure. During the course of review, we noted that the mitigation plan has been implemented.				
Weak or absence of information security design controls	RK0020196	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to instruct Administrative staff to save a job submitter's information on SharePoint (not local computer). The information should be deleted right after the work is completed as it serves only as secondary information. The source of truth (primary information) is stored in PODIO server. If there is a need to keep the information on the local and for a certain period of time per the recommended records retention schedule, the computers/laptops must be encrypted and the backup should be arranged with the department/UBC IT.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

UBC employees and students are given a standard personal information collection notice before they provide their personal information. This discloses the legal authority to collect information, the purpose for collection, and contact information for asking for clarification. It is expected that the job submitters will approach UBC Machine Shop if they have any privacy questions about the use of PODIO. Such questions can be passed along to the PrISM team if necessary.

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

Due to PODIO hosts UBC data on servers located outside of Canada, UBC must secure consent of a participant for this circumstance.

2.5 Consent Withheld Procedure

Job submitters who elect to withhold consent for storage of their information outside of Canada are provided a different choice offered by UBC Machine Shop.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

UBC requires data centers to comply with a detailed set of security requirements. PODIO servers are hosted at AWS Dublin. UBC has relied on publicly available documentation and vendor supplied documentation to establish a level of comfort over the physical security of AWS data centres. The physical security capabilities of AWS data centers meet the UBC standard.

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). Below are implemented controls stated by PODIO:

- Customer-uploaded data is hosted through Amazon Web Services in Dublin.
- HTTPS Encryption on all data between the Podio service and the client web browser. Login without encryption is non-optional. Podio servers are firewalled and only those services which are required to be running are listening. Connections between servers are made using encrypted secure tunnels.
- Podio employees do not access customer uploaded data in Podio without prior customer consent.
- No super-user account exists in the organization. All accounts are private to each individual user.
- Read our privacy policy here: https://www.citrix.com/about/legal/privacy.
- All data is backed up nightly and copied to another off-site location.
- Access all your uploaded data programmatically via the Podio API: https://developers.podio.com/.
- Multiple client libraries available.
- Import/export data or connect external services to Podio via the API.
- Regular security audits are carried out by internal Citrix security team.

However, it was noted that SSL certificate for Machine Shop website (https://technicalservices.mech.ubc.ca/) used for "Job Submission Form" hosting was expired. This practice raises security concerns and is included in the risk mitigation table.

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

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards). The information will be accessed by Machine Shop staff and Shop supervisor for job production and by Administrative Staff for accounting purpose. It is possible that any of the Administrative Staff is making backups and stores the information on their own computers or any location they choose. This practice raises concerns and is included in the risk mitigation table.

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

The data retention and destruction plan has not formally been made available and it is recommended that the project consult with the UBC Records Management Office for the records retention and destruction guidelines. This observation is included in the risk mitigation table.

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

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

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

Information Reviewed	Date Received
CITRIX - Privacy Policy.pdf	2020-07-30 23:51:34
PODIO - Business Continuity Overview Security.pdf	2021-03-04 20:00:18
PODIO - Project Details (internal use).docx	2020-07-30 23:51:01
PODIO - Security Whitepaper.pdf	2021-03-04 20:00:19

6.2 Analysis and Findings

The privacy and security risks were noted during our review. The project has accepted and agreed to implement the remediate actions as per the risk mitigation plan outlined to minimize risk exposures and to comply with FIPPA and UBC Information Security Standards.

6.3 Conditions of Approval

The project to ensure the implementation of the risk mitigation actions during the implementation of PODIO.

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
Markus Fengler

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

Distributed To
Requestor: Bernhard Nimmervoll, Engineering Technician 4- Mech Tech. (Mechatronics **Project Manager:** Bernhard Nimmervoll, Engineering Technician 4- Mech Tech. (Mechatronics) **Owner:** Markus Fengler, Machine Shop Lecturer **Risk Advisor:** Pimkae Saisamorn, Senior Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2020-06-18 21:21:13	2021-03-04 14:48:34