

PIA01919 – PerfectMind

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	2021-01-19	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2021-01-19	Dylan E T Brown	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 1

 1.1 Area Executive Summary..... 1

 1.2 Description of the Program, System, Application, or Initiative Assessed..... 1

 1.3 Scope of PIA 1

 1.4 Related PIAs..... 1

 1.5 Elements of Information or Data..... 2

 1.6 Storage or Access Outside of Canada (including back-ups and recovery) 2

 1.7 Data-Linking Initiative..... 3

 1.8 Is this a Common or Integrated Program or Activity? 3

PART 2: PROTECTION OF PERSONAL INFORMATION 4

 2.1 Personal Information Flow Diagram / Table 4

 2.2 Risk Mitigation Table 6

 2.3 Collection Notice 7

 2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any) 7

 2.5 Consent Withheld Procedure 7

PART 3: SECURITY OF PERSONAL INFORMATION 8

 3.1 Physical Security Measures 8

 3.2 Technical Security Measures..... 8

 3.3 Security Policies, Procedures, and Standards..... 8

 3.4 Tracking Access / Access Controls 8

PART 4: ACCURACY, CORRECTION, AND RETENTION 9

 4.1 Updating and Correcting Personal Information 9

 4.2 Decisions That Directly Affect an Individual..... 9

 4.3 Records Retention and Disposal..... 9

PART 5: FURTHER INFORMATION	9
5.1 Systematic Disclosures of Personal Information	9
5.2 Access for Research or Statistical Purposes	9
5.3 Other Applicable Legislation and Regulations.....	9
PART 6: ACCESS AND PRIVACY MANAGER COMMENTS.....	9
6.1 Information or Materials Reviewed	9
6.2 Information or Materials Not Available for Review	9
6.3 Analysis and Summary	10
6.4 Conditions of Approval.....	10
6.5 Review and Distribution	10

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.....	6

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Area Executive Summary

UBC Kinesiology will implement PerfectMind, a Canadian-based customer relationship management software that uses cloud-based technology to help organizations connect with their users. PerfectMind is a PaaS solution, wherein the organization develops, runs, and manages their operations and databases, while PerfectMind provides the networks, servers, storage, and services to host the application.

UBC Kinesiology will use PerfectMind to manage program registrations and conduct online payments for these services. Specifically, Kinesiology will use PerfectMind to run physical activity programs for children and adults.

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

Registration software for Kinesiology Outreach Programs:

Active Kids: <https://kin.educ.ubc.ca/outreach/active-kids/>

BodyWorks: <https://kin.educ.ubc.ca/outreach/body-works/>

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 PerfectMind, as outlined within this PIA, for use by UBC Kinesiology and its client base.

1.4 Related PIAs

Reference	Description
PIA01473	PerfectMind (Athletics)
PIA01560	PerfectMind (UBC Farm)

1.5 Elements of Information or Data

Personal information (PI) collected by PerfectMind includes name, email address, mailing address, phone number, username and password, payment card number and billing address, IP addresses, browser type, internet service provider, referring/exit pages, operating system, date/time stamp, and clickstream data. PerfectMind also maintains a record of product interests and purchase history.

Device PI is collected via tracking cookies and is combined with self-reported PI to improve site functionality and service offerings, analyze trends, administer the site, track user movements around the site, and to gather demographic information about the user base.

PI collected by Kinesiology includes: Name, gender, birthdate, address, phone, email, emergency contact (name, phone, email and relationship to attendee), personal health information (PHI), medical information about seniors and a doctor's clearance before joining the BodyWorks program, and signature (required on paper forms).

All clients to fill out a Physical Activity Readiness Questionnaire (PAR-Q+) is a common method of uncovering health and lifestyle issues prior to an exercise program starting: <https://educ-kin2016.sites.olt.ubc.ca/files/2019/07/January-2019-ParQplus-updated.pdf> (name, signature, and date are collected on the clearance document, but PHI is not disclosed, it is used only to generate the clearance document).

Parents must complete a minor consent form and waiver to register their children: <https://kin.educ.ubc.ca/outreach/active-kids/faq-policies-and-info-for-parents/>.

Additional details about PI collected:

- Gender is collected for data collection and statistics.
- Birthdate is required to place clients into the appropriate classes based on age (for kids and seniors).
- Email is collected to send out electronic receipts, registration confirmation, liability forms, and serve as a general contact, and for (optional) newsletter subscriptions using CyberImpact (UBC PIA completed).
- Personal health information is collected to ensure seniors have doctor's clearance to participate in fitness programs and personal training sessions. In addition, medical information is collected is required to ensure customized personal training. Many seniors have clinical conditions, so it is necessary to find out what the exact medical conditions and physical abilities before exercises are prescribed, to ensure participants are able to do the movements.
- Payment card information is stored as a digital token in the case of recurring memberships with monthly fees. In all other cases, no payment information is pre-populated for a client. They must enter their card each time they make a purchase.

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

PerfectMind is run on Amazon Web Services (AWS) Canada data centres located in Montreal. There is no storage of data outside of Canada. All collected data will be stored in a Canadian hosting solution. IT and customer support is located in Canada.

All components of the solution are hosted in Canada. The only exception is the "Managed Email Service" which has integration with a third-party vendor powered by Dyn, Oracle. Emails are relayed through their network but no data is retained by Dyn.



1.7 Data-Linking Initiative

<i>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</i>	
1. <i>Personal information from one database is linked or combined with personal information from another database;</i>	No
2. <i>The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;</i>	No
3. <i>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.</i>	No
This project is not considered a data linking initiative as contemplated under s.(36) of FIPPA.	

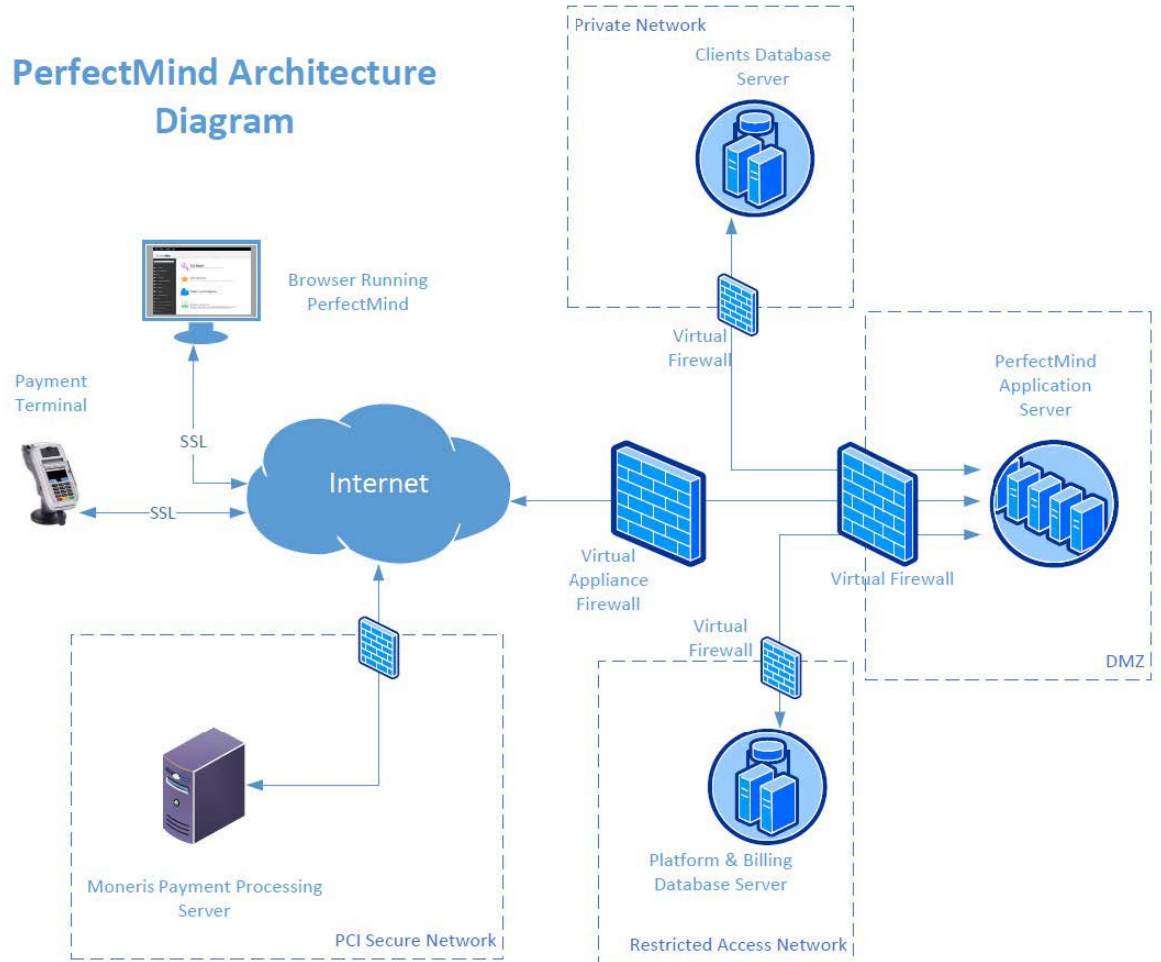
1.8 Is this a Common or Integrated Program or Activity?

<i>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.</i>	
1. <i>Personal information from one database is linked or combined with personal information from another database;</i>	No
2. <i>The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;</i>	No
3. <i>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.</i>	No
This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.	

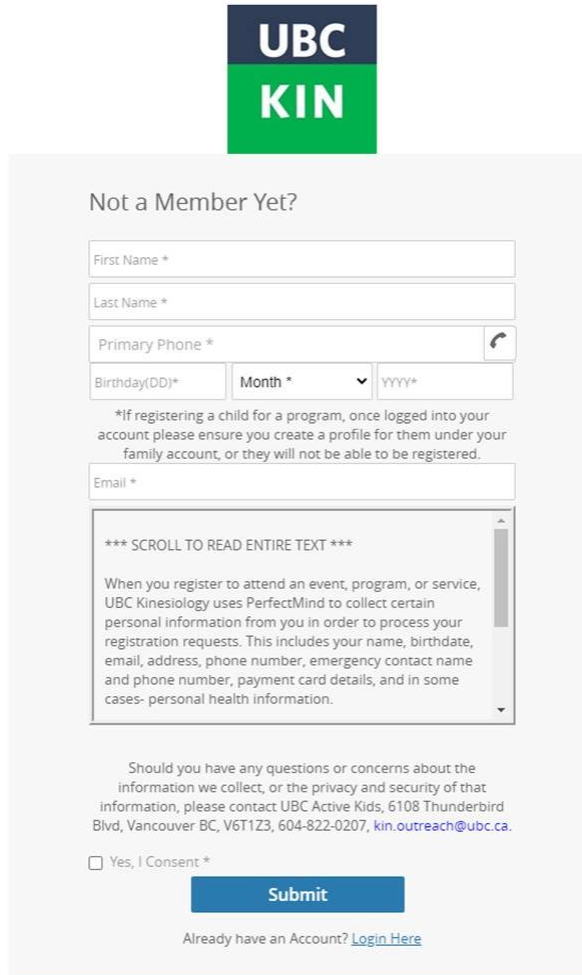
PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

The following diagram documents the information flow through the system architecture:



The following image shows the registration screen:



UBC
KIN

Not a Member Yet?

First Name *

Last Name *

Primary Phone *

Birthday(DD)* Month * YYYY*

*If registering a child for a program, once logged into your account please ensure you create a profile for them under your family account, or they will not be able to be registered.

Email *

*** SCROLL TO READ ENTIRE TEXT ***

When you register to attend an event, program, or service, UBC Kinesiology uses PerfectMind to collect certain personal information from you in order to process your registration requests. This includes your name, birthdate, email, address, phone number, emergency contact name and phone number, payment card details, and in some cases- personal health information.

Should you have any questions or concerns about the information we collect, or the privacy and security of that information, please contact UBC Active Kids, 6108 Thunderbird Blvd, Vancouver BC, V6T1Z3, 604-822-0207, kin.outreach@ubc.ca.

Yes, I Consent *

Submit

Already have an Account? [Login Here](#)

Users register with PerfectMind, create their proprietary login and providing the information required for program registration (dependent on program). Consent to use PerfectMind to collect PI is collected at this stage. Additional PHI is collected from clients in order to modify their training. Clients will be asked to consent to this collection, including consent for minor children, completed online PAR-Q+ clearance forms, and participant waivers, as required (some PI is collected using paper forms).

Steps for PAR-Q+ Completion:

1. Participants navigate to the online PAR-Q+ form and answer health-related questions (survey format): <https://www.healthlinkbc.ca/physical-activity/par-q-and-eparmed-x>.
2. The form does not collect any PI, but rather responses are used the one of two responses:
 - If client answers “no” to all seven questions, then s/he is clear to exercise and can submit the clearance document to Kinesiology for liability purposes.
 - If client answers “yes” to any of seven questions, then s/he needs to go see their doctor to obtain a doctor’s note for physical activity clearance.

During first intake consultation meeting, staff trainers will follow up on any health-related issues. Participants will also review and sign the intake form. Consent to collect and use PI is collected at this state again.

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 controls for volume of personal information	RK0020487	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Policies for the collection and retention of data should be reviewed annually to ensure that the use of PerfectMind does not result in unintended disclosure. PI that is no longer required must be purged at appropriate intervals. Individuals with access to user data must be trained in the handling of PI.				
Inadequate controls for volume of personal information	RK0020501	4 - High	4 - Major	Mitigate	3 – Medium
	Mitigation Plan: PerfectMind has robust access controls to limit disclosure. The unit will implement appropriate to ensure user PI is accessed only by individuals on a need-to-know basis, by users with appropriate access authorities and login credentials. PI must be retained only as long as required to fulfill program registration requirements.				
Disclosing to or allowing unauthorized users access	RK0020624	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Only staff who have been appropriately trained must be allowed to have access to user PI within PerfectMind, and only on a need-to-know basis. Staff contract terms should indicate potential to access client PI.				
Over collection of personal information	RK0020485	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: PI collected must be kept to a minimum, and only that which is required and reasonable to fulfill obligations for managing client relationships, registering in programs and processing payments. No additional use-cases are authorized.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

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

In addition, the privacy policy applicable to all Athletics and Recreation units:

<https://recreation.ubc.ca/home-page/policies/privacy/>.

On registration: When you register to attend an event, program, or service, UBC Kinesiology uses PerfectMind to collect certain personal information from you in order to process your registration requests. This includes your name, birthdate, email, address, phone number, emergency contact name and phone number, payment card details, and in some cases- personal health information. UBC Kinesiology collects this information under the authority of Section 26(c) of the BC Freedom of Information and Protection of Privacy Act (FIPPA). This information will be shared with the UBC School of Kinesiology, event organizers, program/service instructional staff, and UBC's payment processor solely for completion of your registration request. UBC Kinesiology will not share this information with any other parties. Should you have any questions or concerns about the information we collect, or the privacy and security of that information, please contact <name, business title, address, etc.>, kin.outreach@ubc.ca.

On the PAR-Q+ form: You will re-directed to an external non-UBC website to complete your PARQ+ questionnaire. We will be collecting your name and signature upon completion of the PARQ+ questionnaire, but no other personal information. UBC Kinesiology collects this information under the authority of Section 26(c) of the BC Freedom of Information and Protection of Privacy Act (FIPPA). This information will be shared with the UBC Kinesiology, event organizers, program/service instructional staff, and UBC's payment processor solely for completion of your registration request. UBC will not share this information with any other parties. Should you have any questions or concerns about the information we collect, or the privacy and security of that information, please contact kin.outreach@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

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

PerfectMind is hosted at data centers within Canada owned and managed by AWS, which is used for data storage, to store application data and backups. Physical protection of these data centers is managed by the hosting service and is reported in their SOC audits and in other security reports and reviews. UBC privacy staff have relied on documentation made available by Amazon regarding its security measures. In addition, UBC privacy staff reviewed the AWS 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.

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).

The infrastructure and underlying storage used by PerfectMind as well as the clients' databases are using 256-bit SSL encryption. All client data is encrypted during transmission to the AWS Canada datacenters PerfectMind is compliant with Payment Card Industry Data Security Standards (PCI-DSS). Credit card information is fully encrypted and not stored on the account nor the system. That information resides with payment processing company and PerfectMind initiates transaction processing through secure tokenization method.

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).

UBC privacy staff have had limited visibility into or access to PerfectMind's own information security policies, practices, or standards. However, PerfectMind has responded to UBC's Vendor Requirements & Risk Assessment Questionnaire (used when no third party audit certification is present). These responses, in addition to publicly available documentation, assert PerfectMind employs robust standards and practices; however, these assertions could not be substantiated, as PerfectMind 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 AWS are considered robust, meeting and frequently exceeding UBC security requirements.

3.4 Tracking Access / Access Controls

PerfectMind provides a sophisticated profile based permission system. All users of the system will be assigned a profile that limits their access to various functions of the system as well as the data according to the requirements of their position. A limited number of Kinesiology staff (1-10 individuals), on a need-to-know basis, will have access to participant PI for client account management.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

The system provides clients with the capability to update and change their own information.

4.2 Decisions That Directly Affect an Individual

This project does not capture PI that directly affects an individual as contemplated in s.(31)(b) of FIPPA.

4.3 Records Retention and Disposal

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

Per Kinesiology: "If an account holder decided to no longer visit our programs, they may delete their account/information at any time. If a program concludes or a participant withdraws from a program, their account information is still present in our system in case they decide to register again in the future." Kinesiology will build a process where any accounts that have not been active in the previous 12 months are removed. PerfectMind retains all records as long as the UBC Kinesiology account is active.

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 is not related to research and statistical purposes.

5.3 Other Applicable Legislation and Regulations

There are no other applicable legislation or regulations related to this review.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

PerfectMind: Attestation of PCI Compliance, SaaS and Professional Services Agreement (draft), Response to UBC RFP #2016010364, UBC Vendor Requirements & Risk Assessment Questionnaire
Project: Data Flow Inventory, Signed Security and Confidentiality Agreement (UBC Athletics-PerfectMind), PAR-Q+ and Fitness Assessment Forms, Consent form for minors, Participation waiver form.

6.2 Information or Materials Not Available for Review

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 PerfectMind and the associated use-case, as presented by UBC Kinesiology, can be used in the proposed manner in compliance with FIPPA and UBC 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.
- Information is kept secure during transmission and at rest.
- Access to the service requires use of a valid login credentials with appropriate access authorities.
- UBC Treasury validated compliance with PCI-DSS requirements.

Accordingly, PerfectMind can be used as proposed subject to the conditions set out in the following section

6.4 Conditions of Approval

- Any contemplated changes to use of this software that differs from the description provided in this PIA (i.e. collection, use, disclosure or storage of PI) requires a new PIA.
- Any contemplated changes to collection of personal information via PAR-Q+ or similar forms must be discussed with UBC privacy staff.
- Project to develop appropriate training and on/off-boarding procedures to ensure appropriate use of PerfectMind and access to PI.
- Use of social media (e.g. Facebook) for login or any other purposes is not authorized.

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
Amy Kao

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

Distributed To
Requestor: Christian Stockman
Project Manager: Dylan E T Brown
Owner: Amy Kao
Risk Advisor: Christian Stockman

PIA Request History:

PIA Request Date	Report Created
2021-01-18 11:45:49	2021-01-19 11:44:11