PIA01749 – Workday – Finance & Human Resources

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
Johnson, Susan	Safety and Risk Services	Privacy and Information Security Risk Advisor, Major Projects
Lonsdale-Eccles, Michael	Safety and Risk Services	Director PrISM, Safety and Risk Services
Hancock, Paul	Office of the University Counsel	Legal Counsel, Information and Privacy

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
0.10	2018.10.26	Johnson, Susan	PIA Scope initial draft
0.20	2018.12.04	Johnson, Susan	PIA Scope agreed by stakeholders
0.30	2020.07.03	Johnson, Susan	Revised scope due to change to Student timetable, clarify scope vis AEP and related PIAs
0.40	2020.10.08	Johnson, Susan	First draft of complete PIA report
0.50	2020.10.16	Lonsdale-Eccles, Michael	Revised draft
0.60	2020.10.26	Hancock, Paul	Final review/edits
1.0	2020.10.27	Lonsdale-Eccles, Michael	Final draft
1.1	2020.10.29	Lonsdale-Eccles, Michael	Reflect feedback from Executive Sponsors
1.2	2020.11.03	Johnson, Susan	Reflect feedback from CARO

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00		Smailes, Peter Szeri, Dr. Andrew Cormack, Dr. Lesley Mukherjee, Dr. Ananya Buchholz, Marcia	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

TABLE OF FIGURES

PART 1: GENERAL INFORMATION & OVERVIEW

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

The Integrated Renewal Program (IRP) is a multi-year program to transform student administration, human resources and finance business processes and system environments to support UBC's mission and strategic plan. It replaces three legacy systems, the Student Information System (SIS), the Human Resources Systems (HRMS) and the Financial Management System (FMS) at the end of their useful life.

UBC has chosen to partner with and implement Workday as UBC's core administrative platform. It will be used by students, faculty and staff, as an enterprise system that will allow integration and streamlining of complex processes, while remaining easy to use across platforms and devices.

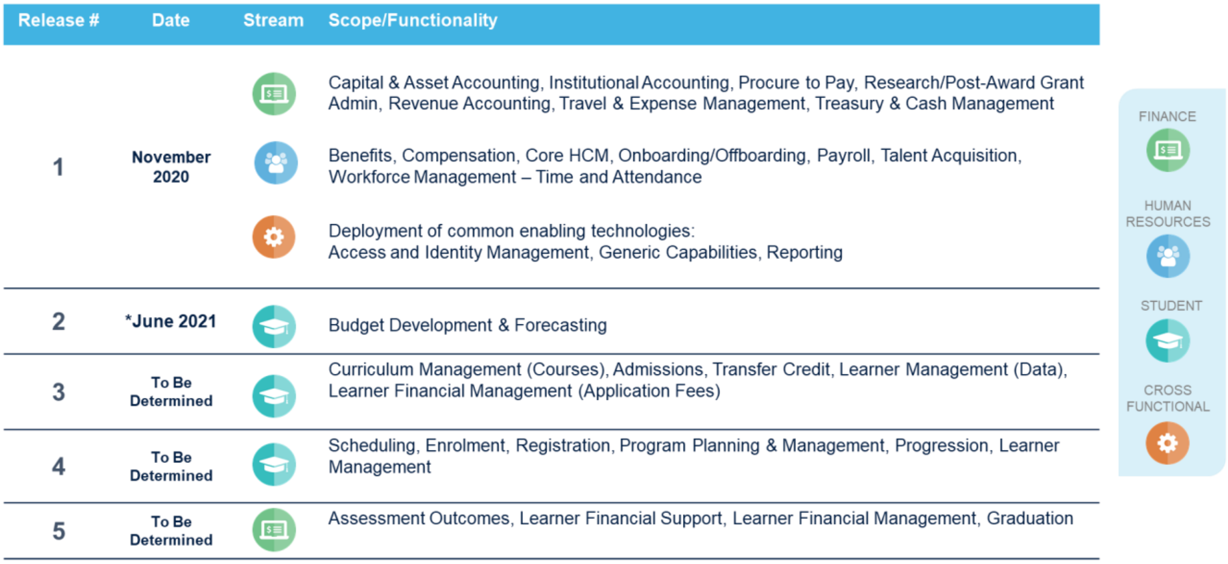
SCOPE OF THE WORKDAY (HR/FIN) IMPLEMENTATION

In November 2020, UBC will replace existing HRMS and FMS systems with either Workday functionality or Point Solutions. See Appendix A – HR/Finance Scope of Business Processes for Finance and Human Resources business processes. There are a number of applications that currently support the functional domains of Human Capital Management (HCM) and Finance. These include:

- Integrated applications that will provide data to Workday and the Point Solutions;
- Enterprise Reporting Data Stores and Enterprise Data Warehouses that will be required for cross-application Strategic Reports and as a data source for analytics;
- The as-is applications, and their technical environment, that will be decommissioned or retrofit as a result of the implementation of Workday.

See Section 1.3 on Related PIAs for details on these applications.

IRP DEPLOYMENT PLAN



Release #	Date	Stream	Scope/Functionality
1	November 2020	💵	Capital & Asset Accounting, Institutional Accounting, Procure to Pay, Research/Post-Award Grant Admin, Revenue Accounting, Travel & Expense Management, Treasury & Cash Management
		👥	Benefits, Compensation, Core HCM, Onboarding/Offboarding, Payroll, Talent Acquisition, Workforce Management – Time and Attendance
		⚙	Deployment of common enabling technologies: Access and Identity Management, Generic Capabilities, Reporting
2	*June 2021	🎓	Budget Development & Forecasting
3	To Be Determined	🎓	Curriculum Management (Courses), Admissions, Transfer Credit, Learner Management (Data), Learner Financial Management (Application Fees)
4	To Be Determined	🎓	Scheduling, Enrolment, Registration, Program Planning & Management, Progression, Learner Management
5	To Be Determined	💵	Assessment Outcomes, Learner Financial Support, Learner Financial Management, Graduation

* Release 2 is being analyzed as the Workday solution has changed with the acquisition of Adaptive Insights

1.2 Scope of PIA

The scope of this PIA is limited to the Human Resources and Finance business processes that will be deployed in November 2020 on the Workday platform. Implementation of Workday Student will require a new PIA. The risks and controls associated with collection, use, access, disclosure, safeguards, retention and destruction of personal information (PI) will be assessed and are the subject of this PIA.

- Finance and HR business processes that collect, use, store and disclose PI (see for details)
- Cross-program processes (e.g. data conversion, security, mobile, training)
- Deployment of common enabling technologies (e.g. reporting)

The PIA is informed by a separate risk assessment of security threats and risks to PI stored within Workday as well as related infrastructure services, including identity and integration services as well as key applications that integrate with Workday. However, the focus of the PIA is on the risks to PI in Workday.

The PIA is informed by document review and discussion with project team members and sponsors.

OUT OF SCOPE

This PIA excludes review of new applications (see 1.3 – Related PIAs):

- Enterprise Maintenance Management System (EMMS)
- Tuition Waiver (Salesforce point solution)
- Integrated Service Center (ServiceNow expansion)
- Education Planner BC (EPBC) provincial shared service
- University Data Analytics Platform (UDAP)

This PIA also excludes review of the processes in regards to reviewing recordings of proctored sessions, as well as reviewing methods students may employ in attempts to defeat the proctoring services in order to cheat on a quiz, test, or examination.

NON-PERSONAL INFORMATION

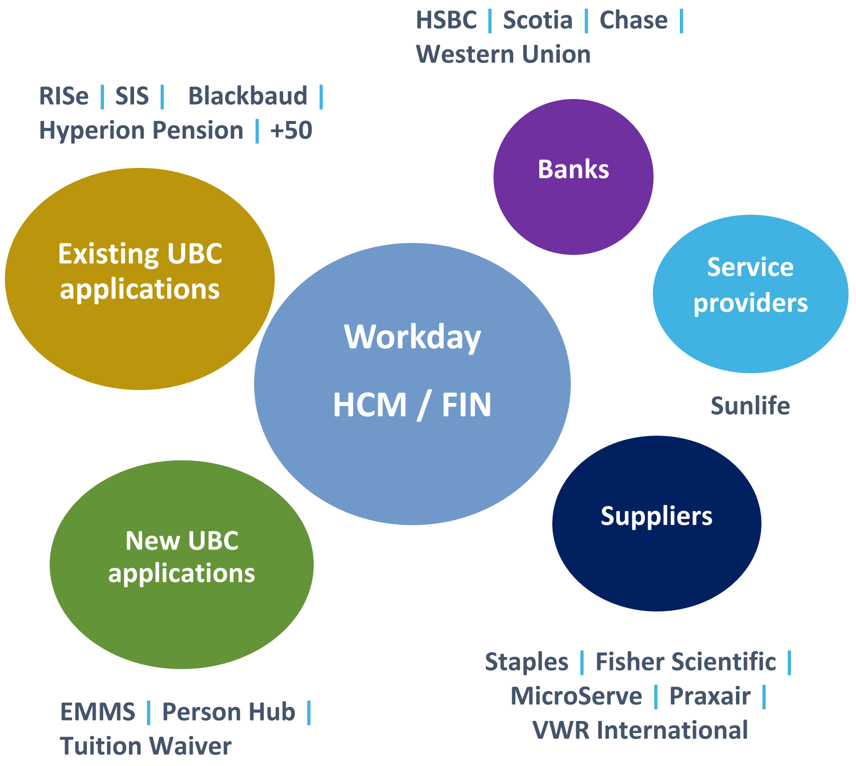
Like all PIAs, this PIA is concerned with Personal Information (PI), which UBC considers to be either High-Risk or Very High-Risk information under the security classification model established in the Security Classification of UBC Electronic Information Standard. Misuse or unauthorized disclosure of this information has a potential for moderate or significant harm to one or more individuals, identity theft, possible severe impact to University reputation or operations, financial loss, such as regulatory fines or damages from litigation. The PIA does NOT assess controls over other information, such as financial information that is not associated with identifiable individuals.

Controls over information beyond PI are assessed separately to this PIA in a related Security Threat Risk Assessment.

1.3 Related PIAs

APPLICATION ECOSYSTEM PROGRAM (AEP) CONTEXT

The scope of the IRP encompasses the core functionality provided by the Workday solution. To provide full functionality required by the University today, there are a number of other applications across the University that exchange data with the existing Finance and Human Resources enterprise systems to access information, report or enable a workflow process.


HSBC | Scotia | Chase | Western Union
RISe | SIS | Blackbaud | Hyperion Pension | +50
Banks
Existing UBC applications
Service providers
Workday HCM / FIN
Sunlife
Suppliers
New UBC applications
Staples | Fisher Scientific | MicroServe | Praxair | VWR International
EMMS | Person Hub | Tuition Waiver

To enable business continuity for any functionality that will not be supported by the Workday platform, existing software applications must be made to work with the new enterprise system (the Workday platform). In addition, and as a part of the transition to Workday, the foundational data model is changing significantly for Finance and HR, leading to the need for updates to the data models or data interchanges for those related applications.

DISPOSITION CATEGORIES

Analysis of the applications conducted in 2019 identified 283 individual applications, which were separated into 'Disposition Categories' for purposes of determining effort required to update and integrate them with Workday. The categories were also used to determine whether privacy assessment work was required and to what extent.

AEP PRELIMINARY RISK ASSESSMENT

Risk classification self-assessment using the UBC Risk Classification Tool was conducted on 23 New and Retrofit Applications (change to existing system in order to integrate with Workday) in October 2019. The assessment focused on PI transmitted to/from Workday and whether the AEP would increase privacy risks. For applications to be decommissioned when Workday goes live, the focus was data conversion risks, controls within the IRP program and on application decommissioning and secure destruction of PI.

APPLICATION ECOSYSTEM PROGRAM ANALYSIS CONCLUSIONS

A number of legacy applications provide PI to Workday or use PI from Workday. We have not assessed the inherent privacy risk in these applications where there is no substantial change to the PI that is being transferred, (i.e. there is no additional privacy risk presented by the Workday implementation).

Privacy Impact Assessments are required for NEW projects, which are NOT included in the IRP PIA. These include:

- Enterprise Maintenance Management System (EMMS)
- Tuition Waiver (Salesforce point solution)
- Integrated Service Center (collection, use disclosure of PI by ISC Helpdesk, including ServiceNow expansion)
- Education Planner BC (EPBC) provincial shared service
- University Data Analytics Platform (UDAP)

Infrastructure projects/services that IRP depends on have undergone Security Threat Risk Assessments (STRAs). These include IAM PersonHub and IEC PersonService/Mulesoft.

In addition, due to potential changes in security caused by retrofitting applications, as well as business criticality of the following systems, Security Threat Risk Assessments (STRA) have been conducted on the following systems:

- Blackbaud CRM
- RISe (Reseach Information Services)
- Pension Administration System
- ePayments
- SIS (changes required for WD implementation and EPBC)

1.4 Elements of Information or Data

The following information and data elements are collected and used for the IRP.

System	High-Level Data
HR	HR module processes PI about workers (e.g. staff, faculty, student workers) who are active or on leave, or those who were terminated or deceased, or are survivors with benefits, within the current fiscal year. For each worker in scope, the following data will be processed: ▪ Bio/Demo data (e.g., names, addresses, visa/permit, SIN, DoB, Self-service) ▪ Organization Data (e.g. Employee ID, organization, location, cost centre, position management) ▪ Job data (e.g. Job profile, employee status, worker type, pay rate) ▪ Compensation data (e.g., base salary amounts, hourly rates) ▪ Benefits data (e.g. plans, groups, eligibility, enrolment, rate tables, integration to benefit provider) ▪ Payroll processing (e.g. time tracking & evaluation, pay calculation, deductions, year-end reporting, integration to house bank) ▪ Current year balances (e.g. tax balances, leave balances, earnings & deduction balances) ▪ Recruitment (e.g. job postings, candidate workflow, onboarding/ offboarding) Other HR transactions may also include PI. See list of HR Business Processes at Appendix A.
Finance	Finance module processes a variety of PI related to financial transactions. The majority of information in these systems is about customers and suppliers, including names, addresses and sometimes SIN #s for suppliers who are sole proprietors. Invoices may contain additional information such as names or addresses of private individuals and details of the services provided, which may be sensitive. Other financial transactions may also include PI. See list of Finance Business Processes at Appendix A.

As may be expected from a complex HR/Payroll system, there are 4,342 data elements in the Worker Object. The full Worker Object report runs almost 300 pages, thus have not included all the data elements in this PIA.

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

All IRP data, including PI, will be stored on servers in Canada. Contract terms between UBC and Workday provide that Workday may only use data centers located in Canada to store UBC Data, including all back-ups thereof. In the event that the AWS Platform in Canada becomes unavailable, Workday may invoke its second-tier disaster recovery procedures and use a back-up of the UBC Data to restore UBC's Tenant(s) in a data center in Dublin, Ireland. This exception for disaster recovery is allowed under section 33.1(1)(p) of FIPPA.

In addition, under the contract between UBC and Workday, Workday has committed to only accessing PI from within Canada, except as required by the IRP and agreed by UBC.

1.6 Data-Linking Initiative

The IRP is not considered to be a Data Linking Initiative, as defined in FIPPA, because it only includes data collected by UBC or its service providers. However, the system will join data from different sources within UBC for use that is consistent with collection.

1.7 Is this a Common or Integrated Program or Activity?

The IRP is not considered to be a Common or Integrated Program as defined in FIPPA because it does not involve:

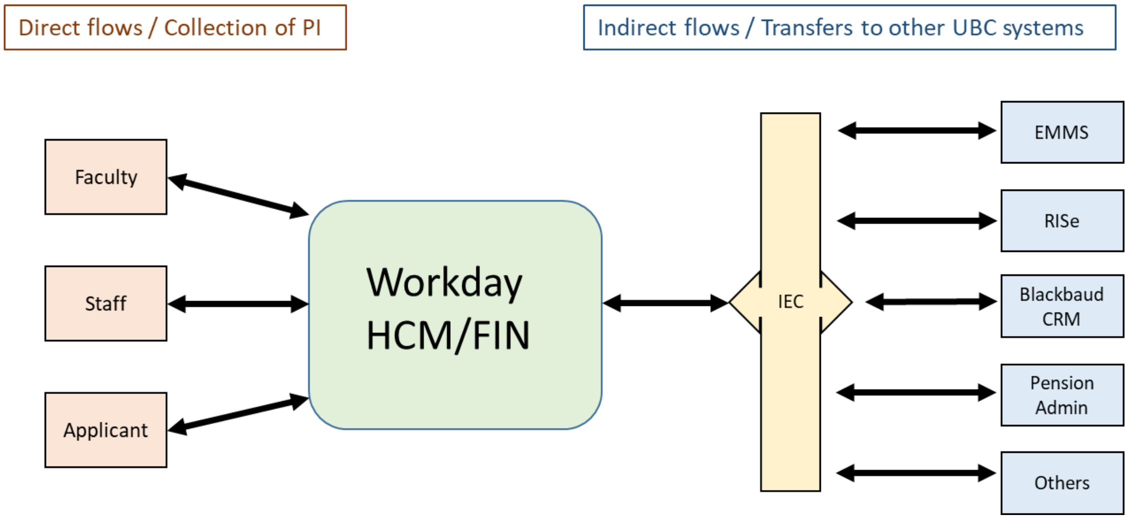
- other public bodies working collaboratively; or
- service provision to one or more other public bodies.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

Personal information contained in Workday is required for UBC operations, specifically HR and Finance business processes. Personal information is collected pursuant to Section 26 of the Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165 ("FIPPA"). The PI will be used, retained and disclosed by UBC in accordance with FIPPA. UBC will not disclose any PI to external third parties unless permitted by law.

To provide full functionality required by UBC today, there are a number of other applications that exchange data with the existing Finance and HR enterprise systems to access information, report or enable a workflow process. In future, these applications will exchange data with Workday via the Integration Enablement Center. For PI exchanged with key systems, this is documented in UBC data flow tools (excerpt in Appendix B). The following diagram is conceptual and abstracts from the number of specific data flows.



2.2 Risk Mitigation Table

The following table identifies the risks to PI that exist in any complex automated system, the controls in place to address those risks, and recommendations based on any observed gaps in controls.

The overall conclusion based on work performed is that all assessed risks are low after considering in-place mitigations. Nevertheless, additional mitigations which will further reduce risk are identified.

	Risk	Description	Mitigation Strategies (including controls in place and recommended)
1	Information security controls protecting Workday are insufficient to protect personal information	The IRP implementation moves critical HR and Finance systems from an aging and vulnerable version of Peoplesoft to Workday and several other new systems/components from reputable vendors, where information security was a key differentiator during selection. The security controls these vendors offer is substantial, and represents a significant improvement from the prior state. The security controls implemented for Workday provide a reasonable level of security for the personal information processed in the system. However, the complexity of information security combined with the scale and complexity of the Workday implementation create a significant compliance challenge. The possibility of an incident affecting personal information is impossible to eliminate.	**IN PLACE** UBC's governance for protection of PI includes: ▪ Information Security Policies, Standards and ▪ Guidelines ▪ Governance bodies with accountability for privacy ▪ and security across UBC ▪ Broad-based privacy and security training ▪ Security technologies ▪ Privacy and security risk assessment and advisory services embedded in the IRP program Workday platform security controls represent a significant improvement from the prior state. Workday undergoes a SOC2 independent assessment on an annual basis encompassing Availability, Confidentiality, Privacy, Processing Integrity and Security. **RECOMMENDED** Recommended mitigations relating to Workday and the supporting ecosystem are described in detail in the STRA and summarized in the Conditions of Approval for this PIA.
2	Disclosing PI not authorized by legislation	Disclosing PI not authorized by legislation or UBC policies exposes UBC to risk of non-compliance with FIPPA and to reputational risk.	**IN PLACE** UBC's governance for protection of PI includes: ▪ Information Security Policies, Standards and ▪ Guidelines ▪ Governance bodies with accountability for privacy ▪ and security across UBC ▪ Broad-based privacy and security training ▪ Security technologies ▪ Privacy and security risk assessment and advisory services embedded in the IRP program Workday platform security controls represent a significant improvement from the prior state. Workday undergoes a SOC2 independent assessment on an annual basis encompassing Availability, Confidentiality, Privacy, Processing Integrity and Security. UBC has policies with respect to disclosure of PI that include sanctions for non-compliance, up to and including dismissal. All project team members have completed online and group training sessions on privacy and security risks and controls. Role based access is place, limiting user access on a need-to know basis. Logging and monitoring capabilities have been developed to deter and detect potential unauthorized access to PI. The Integrated Service Centre will monitor and follow-up alerts. All users will be required to undertake online privacy and security

			training. **RECOMMENDED** The Integrated Service Center should continue to refine access management processes to maintain access control with appropriate approvals, reporting to the Data Security and Roles Committee.
3	Retaining PI longer than necessary may increase the impact of privacy breaches due to the increased volume of information exposed	There is no retention strategy for PI in Workday and associated systems.	**IN PLACE** UBC has retention policies for all HR data (including PI). These are produced in consultation with the Records Management Office. Initial data load into Workday will only include 18 months of history. **RECOMMENDED** Data retention configuration and practices in Workday must be aligned with UBC record retention schedule.
4	PI stored / accessible outside of Canada	Storing information or permitting access to personal information outside of Canada creates a risk of non-compliance with FIPPA and UBC policies and standards.	**IN PLACE** Addressed in the Master Subscription Agreement between Workday and UBC, dated Dec 27, 2017. See Sec 1.3 for more details.
5	PI collected without a privacy notification	Not ensuring that Individuals are aware of why UBC is collecting their personal information, how it will be used and shared, and who they should contact to answer questions about the collection, creates a risk of non-compliance with FIPPA and UBC policies and standards.	**IN PLACE** Appropriate privacy notifications are provided when collecting PI from Faculty, Staff and Students, at the point of initial contact (i.e. recruiting). These notifications have been reviewed and approved by Legal Counsel, Information and Privacy.
6	Over collection of personal information	Collecting more information than is necessary for a program or activity may increase the impact of privacy breaches.	**IN PLACE** Adequate safeguards are in place through functional reviews, data conversion and integration services to ensure that PI collected and stored in Workday, including PI transferred between other UBC systems and Workday, is limited to only that which is necessary for the operation of a UBC Program or Activity.
7	Use of PI for alternate purpose	Using information for purposes other than for which that information was obtained or compiled, or for a use not consistent with that purpose creates a risk of non-compliance with legislation and/or UBC policies and standards and increases reputational harm.	**IN PLACE** All project team members have completed online and group training sessions on privacy and security risks and controls. All users complete online privacy and security training, which covers this issue. Data conversion controls are in place to ensure that transfers of PI to/from Workday comprise the same information as previously transferred to predecessor HR and Finance systems. Role based access limits access to PI for those who do not require access, limiting opportunity for inconsistent use. Access requests to data beyond that to which users usually have access go through UBC's Data Access Framework which assesses if the use will be consistent with the purpose of collection (among other risk factors).
8	Inadequate third-party information sharing controls	Not having appropriate information sharing controls with third parties increases the risk of non-compliance with FIPPA and/or UBC policies and standards.	**IN PLACE** Addressed in the Master Subscription Agreement between Workday and UBC, dated Dec 27, 2017.

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

UBC will collect personal information directly from individuals during the recruitment process. The following is the wording for the collection notice that individuals will see prior to submitting an employment application.

The personal information you provide is collected pursuant to Section 26 of the Freedom of Information and Protection of Privacy Act, RSBC 1996, c. 165 ("FIPPA"). The required personal information is collected for the purposes of supporting and evaluating your application for employment with UBC, for managing your employment relationship with UBC if you are hired, and for aggregate statistical purposes. The personal information will be used, retained and disclosed by UBC in accordance with FIPPA. UBC will not disclose any personal information to external third parties unless permitted by law.

If you have any questions about the collection of information, please contact Human Resources at mailto:hr.info@ubc.ca

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

Not applicable. PI will be stored within Canada.

2.5 Consent Withheld Procedure

Not applicable. Consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Security Policies, Procedures, and Standards

Security of Personal Information is paramount to UBC. For projects, UBC believes that it is important to ensure that privacy and related information security risks are identified as early as possible and that appropriate controls are put in place to mitigate them. Accordingly, privacy and information security risk assessment has been embedded in the IRP program to define appropriate Privacy and Information Security controls that augment the IRP Business Controls.

UBC's holistic view of controls encompasses:

- The platform (protected by Workday and AWS)
- The architecture and configuration (controlled by UBC)
- The operational processes put in place to maintain security
- The security culture and environmental protections
- Protection of PI throughout the project

The Privacy and Information Security Risk & Controls Matrix (PrIS-RCM) is an assessment tool that was developed to support the program teams in identifying and mitigating risks.

Confidentiality, Integrity and Availability of data have all been assessed **however, the priority has been the Confidentiality of Personal Information.** Risk assessment has covered the following security elements:

- **Security access** - Physical and logical security restricting access to data (especially Personal Information) in the new IT environment, access and password controls to the database and operating system, and sensitive access.
- **Data migration and conversion controls** - processes and activities to verify that Personal Information is converted from legacy systems SIS (Student), HRMS (HR) and FMS (Finance) in a controlled, complete, accurate and privacy-protective manner.
- **Interface controls** - aim to ensure that the PI transferred between systems is encrypted (where appropriate); recoverable and auditable.
- **IT controls** - procedures and activities to protect the confidentiality of Personal Information within the overall IT environment (i.e. database, IT infrastructure, operating system and network environment).
- **Change management** - Integrity of the IT Environment through Change Management procedures over the Workday application, operating system and database on which solution resides.
- **Business intelligence and reporting controls** - those processes and activities to verify that reports do not result in inappropriate use or disclosure of Personal Information.

The results of the security risk assessment work have informed the PIA, specifically the Risk Mitigation Table in Section 2.2.

This review has relied on the SOC2 Type II for assurances with respect to the Workday platform in Canada.

In our opinion, the security controls implemented for Workday provide a reasonable level of security for the personal information processed in the system.

See the Security Threat Risk Assessment for observations and recommendations with respect to security controls and an overview of critical controls in place.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Workday functionality will allow all system users to update their own information directly into the system through the ‘employee as self’ functionality. Changes are subject to validation by UBC HR and Finance staff. For example, changes to banking information may require confirmation to reduce potential impact from phishing/credential theft.

4.2 Decisions That Directly Affect an Individual

Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Personal information is collected for the purposes of supporting and evaluating the individual’s application for employment with UBC. If they are hired, additional PI is collected for purposes of managing the employment relationship with UBC.

If you answered “yes”, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Individual users will be able to update much of their own information directly into the system, subject to validation.

4.3 Records Retention and Disposal

If you answered “yes”, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

The UBC Records Management Office provides a unified approach to records management, supports overall effective information management, and leads the transition to electronic records management at UBC in an efficient, secure, and sustainable manner.

UBC’s current retention policies can be found at https://recordsmanagement.ubc.ca/schedules/

Data converted into Workday includes 18 months of faculty and staff data. Data retained in UBC’s legacy systems will continue be managed according to the HR retention schedule. Going forward, configuration and practices in Workday must be aligned with UBC’s retention policies and schedules.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No. UBC will share personal information stored in the Workday system with UBC's service providers (e.g. an individual's banking information to its house bank to pay staff). UBC also transfers information as required by federal and provincial statutes (e.g. payroll information to CRA). However, UBC does not believe these to constitute "systematic disclosures".

5.2 Access for Research or Statistical Purposes

Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No. Any release of information for research purposes would either be aggregated/anonymized or be subject to consent prior to release. This is managed by the Data Access Framework under the auspices of Enterprise Data Governance.

Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FIPPA. Under this same section, this information is required to be published in a public directory.

No.

5.3 Other Applicable Legislation and Regulations

Legislation beyond FIPPA have not impacted this PIA.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

DISPOSITION CATEGORIES

Many individuals in the IRP and AEP program teams and UBC IT have contributed to the information included in this PIA, including the following:

- Chris Mercer (IRP Program Director)
- John Thomson (AEP Program Director)
- Paul Hancock (Legal Counsel, Information and Privacy)
- Michael Lonsdale-Eccles (Director of PrISM, Safety & Risk Services)
- Corinne Pitre-Hayes (Director, Application Sustainment and Solution Architecture)
- Harjot Guram (Director, ISC Operations)
- Paul Roberts (Director, SD&D – Deloitte)
- Don Thompson (Chief Information Security Officer)
- Marcela Hernandez (Chief Data Officer, Data Governance)
- Jennifer Kain (Chief Audit and Risk Officer)
- Leisa Belanger (Director, Transformation Finance)
- Samantha McLaughlin (Director, Transformation HR)
- Sharon Rashtian (Senior Manager - Security)
- Feng Liang (IRP Solution Architect)
- Laleh Mosadegh (Associate Director, IEC)
- Gary Kupecz (Project Manager, IEC)
- Luca Filipozzi (Enterprise Architect)
- Jennifer Burns (Associate Vice President, Chief Information Officer)
- Larry Carson (Associate Director, Information Security Management)
- Aaron Heck (Senior Manager, IT Solutions Security and Architecture
- Zoe Armer (Program Manager, Security)
- Sebastian Gonzalez (Senior Manager, Identity and Access Management)
- Hari Mailvaganam (Identity and Access Management)
- Elaine Zhao (Identity and Access Management)
- Keith Fraser (Workday)
- David Marshall (Deloitte)

DOCUMENTS REVIEWED

- IRP Program Charter V7
- Logical Security Architecture
- IRP Security Strategy and Plan
- IRP functional requirements
- IRP non-functional requirements
- IRP User Access Framework
- IRP Mobile Security Strategy and Framework
- UBC Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
- UBC Information Security Standards
- UBC Cybersecurity Practice Guide
- Workday Enterprise Security Overview
- Workday Security and Data Privacy
- Workday Security SOC2 document (most recent dated Sep 20, 2019)
- Workday Mobile Security FAQ
- UBC data anonymization tool documentation
- Person Hub documentation
- IEC website

6.2 Information or Materials Not Available for Review

UBC is not aware of any requested materials that were not available for review.

6.3 Analysis and Decision

This Privacy Impact Assessment has determined that, provided the conditions listed below are implemented, the services in scope can be delivered in compliance with FIPPA and reasonable compliance with UBC policies.

6.4 Conditions of Approval

The following conditions apply:

1. Recommendations outlined in the Security Threat Risk Assessment, pertaining to Workday and information security sustainment, are reviewed and actioned where appropriate
   A. Risk assessment activity should continue to complete scope for this release.
   B. Detailed gaps identified need ownership assigned for further action.
   C. Given the scope, complexity and risk, a post implementation review commencing spring/summer 2021 is recommended. The scope is to be determined, but at a minimum should cover:
      - confirming agreed gaps have been mitigated
      - evaluate emerging/undiscovered risk
      - evaluate maturity of the Integrated Service Center, and related internal service providers ability to sustain information security

2. Recommendations outlined within this PIA are reviewed and actioned where appropriate
   A. The Integrated Service Center should continue to refine access management processes to maintain access control with appropriate approvals, reporting to the Data Security and Roles Committee.
   B. Data retention configuration and practices in Workday must be aligned with UBC record retention schedules.

APPENDIX A: HR/FINANCE SCOPE OF BUSINESS PROCESSES

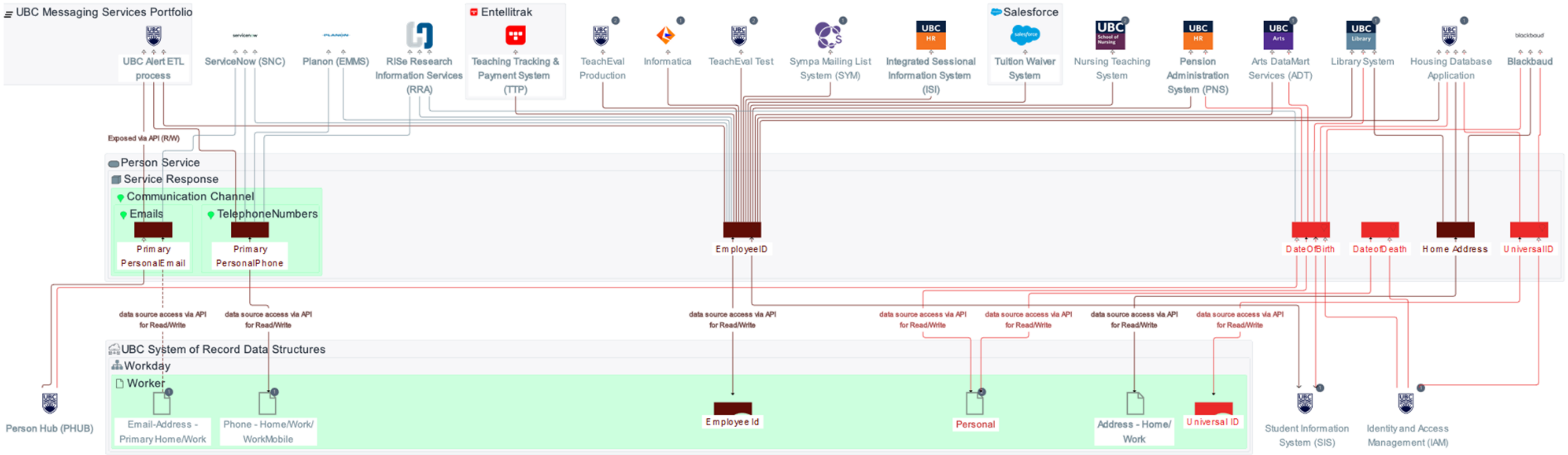
	HCM Functional Area	Solution	Description
1	Core HR Management	Workday	This area focuses on core information related to the institution and to the employee, including the broader workplace (i.e. Paymaster). It includes: organizational charts, employee records (personal information, work history, bios, interests and affiliations, status and location), position management, and self-service options for employees to view, access and where appropriate, submit changes to their information.
2	Compensation	Workday	Compensation programs and policies are in alignment with the Public Sector Employers Council (PSEC) and provide monetary compensation to support retention and attraction of staff and faculty, as well as rewards sustained performance. The programs and processes include: job evaluation and classification, compensation reviews, market surveys, and salary administration (i.e. faculty salary increases, honoraria, administrative stipends, merit increases, step increases, general wage increases, etc.).
3	Benefits	Workday	Benefits are a foundational component of a faculty and staff's total compensation package. The program includes health benefits such as: MSP, Extended Health, Dental, Health Spending Account, Employee & Family Assistance Program, Life Insurance, Long-term Disability Plan, etc., as well as delivery of administration of benefits (including rate changes, retroactive enrolment, adjustment and termination of benefits)
4	Payroll	Workday	UBC has a robust payroll function that supports timely and accurate payment of staff, faculty and Paymaster individuals represented by numerous bargaining units and employee groups. It includes managing the payroll cycle, which includes calculation of pay, taxes and deductions, payroll processing, year-end reporting. etc.
5	Talent Acquisition	Workday	This area supports the attraction, interviewing and hiring of internal and external applicants to roles within the university. It involves external advertising, job postings, application criteria and packages, recruitment methodology and candidate assessment/selection, selection committees, and offers. It also included compliance with regulatory requirements (i.e. visa and work permits).
6	Onboarding/Offboarding	Workday	Onboarding supports the hiring process by which new or existing employees are welcomed into the university and/or Faculty/VP Unit/Department, and acquiring the necessary information, tools and learning to be effective in their new role. Offboarding supports staff and faculty when they leave the university or their role by providing the necessary information and tasks prior to their departure date.
7	Workforce Management	Workday + Point Solution	Workforce management encompasses two distinct areas: workforce scheduling, and workforce time and attendance. Combined it includes the proper forecasting and scheduling of employee resources while ensuring accurate usage, tracking and reporting or time, attendance and leaves. It brings an aligned and coordinated approach to employee resourcing and deployment within UBC's complex work environment (i.e. numerous business rules, collective agreements, various jobs and locations, etc.) while ensuring compliance with regulatory requirements.

	FIN Functional Area	Solution	Description
1	Capital and Asset Accounting	Workday	Process for accounting treatment of UBC Capital expenses including clarifying distinction between operating expenditures and capital expenditures, fair allocation of the cost of capital assets against revenues over the useful life of the asset, tracking the asset, and managing the full accounting life cycle of large and small-scale capital assets.
2	Asset Installation and Maintenance	Point Solution	This includes tools to determine the development, acquisitions of new assets, replacement, dispositions and health checks/maintenance on existing assets from an operational and financials perspective.
3	Institutional Accounting	Workday	This includes integration to all financial sub-ledgers, budget development, supply chain, HR and payroll. Areas of focus include general ledger, chart of accounts, fund accounting, journal entries and the management of period and year-end close.
4	Procure to Pay	Workday	This includes the management of supplier master data, the maintenance of supplier catalogues, the creation of requisitions and purchase orders, the receipting of goods and services and the payment of supplier invoices. Areas of focus include eProcurement, dynamic discounting and contract management in order to maximize value to the organization and to enhance the user experience.
5	Research/Post-Award Grant Administration	Workday	Post-award activities are those processes and activities that take place after the grant, contract, or cooperative agreement has been awarded to the university. This includes the operational administration of the grant, including monitoring the research budget and cash received, maintaining compliance to sponsor restrictions, sponsor billing and reporting activities.
6	Endowment Accounting	Workday	Endowment accounting is the administration around the establishment of endowments from donors, distribution of income and gains to endowment accounts, management of funds to ensure that restrictions and parameters as defined by donors are adhered to and reported on effectively.
7	Project Accounting	Workday+ MS Dynamics NAV	This includes enabling the process around managing projects holistically across the university which includes creation, management of resources and spend across projects.
8	Revenue Accounting	Workday	This area focuses on external billing and customer records, including collections, cash and electronic receipts and deposits, customer management and analytical information.
9	Travel & Expense Management	Workday	The systems deployed by a business to process, pay, and audit employee-initiated expenses. These costs include, but are not limited to, expenses incurred for travel and entertainment.
10	Treasury & Cash Management	Workday + FIS Integrity	Treasury management includes processes such as closing individual active risk management transactions, management of daily cash flows including investment of surplus balances, the preparation and execution of financing and capital measures in consultation with the banks and maintaining relations with those banks, and administration of internal loans. Closing transactions involves settlement and account booking processes.
11	Inventory	Planon	Inventory management is the supervision of non-capitalized assets (inventory) and stock items. A component of supply chain management, inventory management supervises the flow of goods from manufacturers to warehouses and from these facilities to the points of consumption. Inventory management in this context is for non-point of sale systems.
12	Work Orders	Point Solution	This area focuses on core information related to the institution and to the employee, including the broader workplace (i.e. Paymaster). It includes: organizational charts, employee records (personal information, work history, bios, interests and affiliations, status and location), position management, and self-service options for employees to view, access and where appropriate, submit changes to their information.

APPENDIX B: PERSONAL INFORMATION FLOW DIAGRAM

INDIRECT FLOWS OF PERSONAL INFORMATION BETWEEN WORKDAY AND UBC SYSTEMS VIA IEC PERSONSERVICE

The diagram below has been excerpted from UBC's data flow diagramming tool / repository and is filtered to display only select PI.


UBC Messaging Services Portfolio
UBC Alert ETL process
ServiceNow (SNC)
Planon (EMMS)
RISe Research Information Services (RRA)
Entellitrak
Teaching Tracking & Payment System (TTP)
TeachEval Production
Informatica
TeachEval Test
Sympa Mailing List System (SYM)
Integrated Sessional Information System (ISI)
Salesforce
Tuition Waiver System
Nursing Teaching System
Pension Administration System (PNS)
Arts DataMart Services (ADT)
Library System
Housing Database Application
Blackbaud
Exposed via API (R/W)
Person Service
Service Response
Communication Channel
Emails
TelephoneNumbers
Primary PersonalEmail
Primary PersonalPhone
EmployeeID
DateOfBirth
DateofDeath
Home Address
UniversalID
data source access via API for Read/Write
data source access via API for Read/Write
data source access via API for Read/Write
data source access via API for Read/Write
data source access via API for Read/Write
data source access via API for Read/Write
data source access via API for Read/Write
UBC System of Record Data Structures
Workday
Worker
Person Hub (PHUB)
Email-Address - Primary Home/Work
Phone - Home/Work/ WorkMobile
Employee Id
Personal
Address - Home/ Work
Universal ID
Student Information System (SIS)
Identity and Access Management (IAM)