PIA01514 — DAE Snowflake

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

DAE Data Governance and DAE IT is exploring Snowflake as a data platform for data analysis and warehousing capabilities. The project is structured in phases to evaluate the platform's capability and efficiency, with an initial planning and set-up phase, followed by a proof-of-concept testing phase, and concluding with an analysis of performance metrics. A business case will then be developed to aid the Project Sponsor in making a decision regarding to what extent the Snowflake platform has achieved the objectives in a cost-efficient manner.

Snowflake, a multinational corporation, has offices around the world. Snowflake servers are hosted at Amazon Web Service (AWS) in Canada. Snowflake is not integrated with any systems nor CWL integration at this stage. Data files are extracted to .csv format from UBC Blackbaud CRM and are manually uploaded to Snowflake staging by DAE IT team.

1.2 Project Description

The project aims to leverage cloud-hosted solutions to address resource and compute limitations and improve data processing capabilities. This will offer greater scalability, as well as the ability to quickly model solutions without having to remodel UBC-hosted infrastructure to support new initiatives. This is also in-line with UBC's Architecture Review Board (ARB)'s guiding principles and cloud-first strategy. DAE is exploring Snowflake for this use, in hopes that it could help us derive quick insights and draw previously unknown relationships in our data.

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

A review of privacy and security controls for the new data platform during the trial phase.

1.4 Data Elements

The platform will handle standard constituent information necessary for operational and analytical purposes, adhering to privacy regulations.

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

All project data will be hosted and managed within Canada, in compliance with national data residency requirements.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under FIPPA s. (36). The project does not involve combining data from multiple sources.

1.7 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in FIPPA Schedule 1.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram/Table

None provided.

2.2 Risk Mitigation Table

Privacy Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Retaining PI longer than necessary	RK0020750	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: UBC data stored on Snowflake servers for testing must be permanently deleted after the testing is completed. It is recommended the project arrange for data destruction with Snowflake and request a certificate of destruction.				
Unauthorized access to PI during design and development	RK0020748	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: The project indicated a need of production data be used for testing in the test environment to ensure Snowflake works and suits the business needs. It is recommended that the same security controls be implemented in the test environment as in the production environment and to comply with UBC Information Security Standards.				
Lacking Third Party legal agreements for information sharing	RK0020747	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project has arranged the mutual non-disclosure agreement to be signed by UBC and Snowflake prior the PoC work started. However, if the project would like to further proceed with the full implementation of Snowflake, a contractual agreement with Snowflake must be made available and covers the following key privacy provisions: Personal information collected without authorization; Personal information stored in Canada; Personal information disclosed without authorization; and Personal information not stored long enough / too long.				
PI stored / accessible outside of Canada	RK0020751	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Snowflake's software support team may be acquired from outside Canada. This raises a concern over disclosure of PI outside Canada and may violate the FIPPA s.33.1(1)(p).The project to ensure that practices below are followed otherwise a consent from an individual will be required: • the supports be limited only for installing, implementing, maintaining, repairing, trouble-shooting or upgrading of Snowflake as well as data recovery from system failure; and • a temporary access be granted within the minimum period of time necessary to complete such supports. Any on-going access should not be given.				

Security Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020749	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project to ensure that the following security controls are in place: • All data is encrypted at rest and all communications between UBC and Snowflake is encrypted via SSL. UBC data is transmitted over Transport Layer Security (HTTPS) to Snowflake and data stored in Snowflake database is encrypted with AES 256-bit encryption. • A password authentication is implemented when accessing Snowflake. Snowflake connector, tool and database must be implemented with the password that is complied with the UBC Password Standard, e.g., a minimum of10 characters long with complexity.				
Weak or absence of information security design controls	RK0020752	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: A formal security matrix/plan is not developed during the PoC phase however the project evaluated the security capabilities and methods to segregate, manage, and leverage data. However, if the project would like to further proceed with the full implementation of Snowflake, it is recommended that a formal security matrix or plan be developed to ensure a proper segregation of duties and need-to-access basis are followed.				

2.3 Collection Notice

Donors and Alumni should be 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.

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

Consent is not required for as this project does not result in the storage of personal information outside Canada. Given the followings practices are met:

- the supports be limited only for installing, implementing, maintaining, repairing, trouble-shooting or upgrading of Snowflake as well as data recovery from system failure; and
- a temporary access be granted within the minimum period of time necessary to complete such supports. Any on-going access should not be given.

2.5 Consent Withheld Procedure

Consent withheld procedures are not required as consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

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

3.2 Technical Security Measures

UBC has several information security standards that set out the minimum requirements for the protection of personal information. Below are implemented controls stated by Snowflake:

- Snowflake's Risk Management Process is modeled on NIST 800-56 Tier 3 and is performed at least annually.
- Access to the systems and infrastructure that support the Snowflake Service is limited to authorized personnel and requires multi-factor authentication (MFA). There are no actions that can be performed without identification and authentication.
- User access to the systems and infrastructure that support the Snowflake Service is reviewed quarterly.
- Snowflake maintains a current listing of all authorized personnel with access to systems and infrastructure that support the Snowflake Service.
- Passwords are constructed in accordance with minimum standards for length, complexity, and non-reuse of previous passwords. - All Customer Data is considered Restricted and is encrypted in transit over untrusted networks, and at rest.
- Snowflake personnel do not have access to Customer Data in unencrypted form. Exceptions require prior written customer approval and access is temporary.
- Access to networks and systems required to operate and manage the Snowflake Service requires initiating a secure connection via an approved method (i.e., VPN) and MFA.
- Snowflake leverages IaaS security group policies to enforce its firewall policies which are configured to restrict traffic to Snowflake-required network protocols. The policies are reviewed regularly.
- As part of on-boarding, new hires complete initial security and training, sign a proprietary information agreement, and digitally sign the information security policy that covers key aspects of this policy and Staff Personal Data Handling & Responsibilities Policy.
- Events identified are logged and collected in a central system and protected from tampering. Logs are stored for six months, 12 months, and to two years depending on the security monitoring application.
- Encryption algorithms or methods must be consistent with NIST guidelines. Snowflake manages customer keys on behalf of customers unless customer provide their own account encryption keys.
- Vulnerability scans are automatically performed weekly on systems required to operate and manage the Snowflake Service. The vulnerability database is updated regularly.
- Snowflake patches systems based on Snowflake-defined risk criteria, including applicability and severity.
- All software changes must adhere to the Committing Code Policy and to the Code Review Policy.
- Snowflake conducts security assessments of IaaS providers no less frequently than annually.

The project indicated a need of production data be used for testing in the test environment to ensure Snowflake works and suits with the business needs. It is recommended that the same security controls be implemented on the test environment as in the production environment and to comply with the UBC Information Security Standards.

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

The project is storing the extracted data (from Blackbaud CRM) on DAE IT shared network drive. Permissions to access this folder and Snowflake are granted based on development and testing roles following proper segregation of duties. However, if the project would like to further proceed with the full implementation of Snowflake, it is recommended that a formal security matrix or plan be developed to ensure a proper segregation of duties and need-to-access basis are followed.

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

This project is required to comply with UBC Records Management Policies. UBC data stored on Snowflake servers for testing must be permanently deleted after the testing is completed. It is recommended that the project arrange for data destruction with Snowflake and request for a certificate of destruction.

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 does not involve the disclosure of personal information for research or statistical purposes as contemplated under FIPPA s. (35).

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

Overall provided information was deemed reasonable to provide an understanding of operating privacy and security controls built within and around Snowflake and allow us to assess the mitigated risks and recommend the risk mitigation plan to ensure that the residual risks are at an acceptable level.

6.2 Analysis and Findings

Our review noted the key privacy and security risks and the risk mitigation plan is recommended and provided to the project. The project has agreed to implement the recommended remediate actions as outlined in the risk mitigation plan to minimize risk exposures and to comply with the FIPPA requirements and UBC Information Security Standards.

6.3 Conditions of Approval

This PIA is conducted serving the Proof-of-Concept (PoC) for Snowflake. It is the project's responsibility to implement the recommended risk mitigation actions upon the PoC setup and ensure that it complies with the FIPPA requirements and UBC Information Security Standards. If the project wishes to further proceed with the full implementation of Snowflake, a new PIA submission will be required.

6.4 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

Assessment Acceptance
George Firican

Distribution
Requestor: Pradeep Nair, Managing Director, Advancement Services **Project Manager**: George Firican, Director, Data Governance &Business Intelligence **Owner**: George Firican, Director, Data Governance & Business Intelligence **Risk Advisor**: Pimkae Saisamorn, Senior Information Security Risk Analyst

PIA Request Submission	Report Completion
2022-10-27	2020-06-02