VANCOUVER ISLAND UNIVERSITY

Privacy Impact Assessment for:

Information Technology Services: Airtable (Formagrid Inc.)

Contents

Part 1 – General

Name of Department:	Information Technology Services		
PIA Drafter:	Janelle LaCroix/Mike Culbertson		
Email:	pia@viu.ca	**Phone:**	
Program Manager:	Omair Quraishi		
Email:	omair.quraishi@viu.ca	**Phone:**	

1. Description of the Initiative

Airtable is a cloud-based platform that allows users to organize, record, and integrate data by way of linked relational databases. Users can pull and sync data from Google Sheets, Excel, social media sties and various other apps. However, the intention of the proponent is to use this SaaS solution to create dynamic organizational charts for the Information Technology Services (ITS) team, which would include pulling existing VIU employment data from HR databases as well as manual data entry. Future applications for the software may include incorporating results of Strengths' Finders assessments for each member of the IT team, as well as entering dietary considerations for ITS employees for the purpose of inter-department event planning.

2. Scope of this PIA

To examine the risk of FIPPA non-compliance when Airtable is used in a manner that involves the collection, use, and retention of personal information. This PIA covers the use as described above;

any further uses, especially that involve third-party integrations, will need either a new PIA or an addendum to this document. This PIA does not cover Strengths' Finder program.

3. Related Privacy Impact Assessments:

There are not directly related PIAs within VIU.

4. Elements of Information or Data

Information Type	Information Collected
Personal Information	**From Students:** N/A **From Third Parties:** N/A **From VIU Employees:** Employee number, position number, photos and possibly dietary information. For the managers with editing access, usernames and passwords would be created for account registration and creating staff profiles.
Other information (This info is not personal per se, but when combined can create more sophisticated profile of individuals).	**From VIU Employees:** supervisor info, role they report to, pay band, bargaining unit, seniority info, work order they are assigned to, and campus location.
Contact details	**From Students:** N/A **From Third Parties:** N/A **From VIU Employees:** Full Name, work Email, and work phone number as well as position/job title.
Account information	N/A
Commercial information	Standard VIU business information would be shared to facilitate the purchasing transaction.

*If personal information **is** involved in your initiative, please continue to the next page to complete your PIA.*

*If **no** personal information is involved, please submit Parts 1, 6, and 7 unsigned to fippa@viu.ca. A privacy advisor will be assigned to your file and will guide you through the completion of your PIA.*

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada: Yes: Airtable's servers are in the United States of America (USA) as well as subprocessors that store data in other countries; see below.

6. Sensitive Personal Information: Does the project/initiative involve very sensitive personal information? Examples of sensitive personal information include personal health information, genetic and biometric data, personal financial information, geolocation data, criminal records, counselling records, HR records and payroll records. **If so, will the sensitive personal information collected be stored outside of Canada?**

The project will include collecting and storing **Sensitive Personal Information** in the form of employment and payroll information such as: employee number, position number, staff photo (if available).

Airtable's servers are located in the USA and hosted using US-based AWS servers (US-East-1). In addition, Airtable uses several subprocessors located primarily in the USA (and in some instances Germany, Honduras, Romania, and the Philippines) for hosting customer data and for providing the core infrastructure for service delivery. Airtable has policies in place that ensure that all subcontractors with any access to customer data are bound by strict Non-disclosure Agreements (NDAs) and adhere to data protection requirements from Airtable's customers.

7. Data-linking Initiative*

This is not considered a data-linking initiative as contemplated in s.36.1 of FIPPA.

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	
If you have answered "yes" to all three questions, please contact the Privacy Officer at privacy.officer@viu.ca to discuss the requirements of a data-linking initiative.	

8. Common or Integrated Program or Activity*

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

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
This initiative involves a program or activity that provides a service (or services);	

Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies.	
The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

9. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table				
	Description/Purpose	**Personal Information**	**Type (Collection, Use or Retention)**	**FIPPA Authority**
1.	Create organizational chart	The administrator will use existing Human Resource data to populate the software such as: Full Name, Work Email, Position/Role, Role they Report to, Supervisor info, seniority information, pay band, location the serve in (campus'), employee number, position number, photo, FTE information, bargaining unit, work-order they are assigned to	Collection, Use, Retention	Section 26 (c) and (e)
2.	Dietary Restrictions	Dietary restrictions could include health info such as allergies and diabetes, for example.	Collect, use, retain	

10. Risk Mitigation Table

Risk Mitigation Table				
	Risk	Mitigation Strategy	Likelihood	Impact
1.	Unauthorized access by VIU employees	Airtable has security features that restrict access such as:	Low	Medium

		- collaborator permissions – controls who you share a workspace with and whether they can modify content. - restriction to Airtable views through password-protected share links or email domain. -Two-factor authentication (2FA) -Revision history of any modifications to records		
2.	Linking to external databases such as social media sites that contain personal information that VIU does not collect or need to collect (such as Facebook relationship statuses). - Facebook integration allows you to create a new post on a connected FB page.	Airtable does not support posting to personal profiles, only to pages, so there would not be any interlinking of people's personal Facebook profiles.	Low	High
3.	Unauthorized access by Airtable employees	Airtable uses IAM (Identity and Access Management) to manage users who have access. Access permissions for all systems (tools, apps, databases, operating systems, etc.) incorporate the principles of separation of duties and least privilege. This means tasks can only be completed with the participation of more than one employee, and that employees have the minimum privileges needed to perform actions.	Low	Medium
4.	Data breach	Airtable meets high international standards for security compliance, including GDPR: "Airtable is SOC 2 Type 2 and ISO 27001 certified. Airtable is also GDPR, PCI SAQ-A, and CCPA compliant. Further information can be found at: https://www.airtable.com/security. In the event of a security or privacy incident, Airtable notifies any affected users of a breach. Incidents are	Low	High

		classified by severity levels, and there are procedures to collect and maintain a chain of custody for evidence during an incident investigation.		

11. Collection Notice:

The personal employment information has already been collected by VIU for employment purposes. The intended use of the PI by the proponent – to build an organizational chart - is consistent with the purpose for which the information was collected and for operating the ITS department. Therefore, a collection notice is not necessary for this project.

Part 3 – Security of Personal Information

12. Please describe the physical security measures related to the initiative (if applicable).

[redacted]

13. Please describe the technical security measures related to the initiative (if applicable).

Airtable's security program aligns with and is **certified** by SOC 2 Type 2 and ISO 27001 guidelines.

[redacted]

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

s. 15(1)(l)

Utilize Airtable access security features such as:

- [redacted]

15. Please describe how you track who has access to the personal information.

The proponent (Chief Information Officer) will assign access parameters to ITS management using Airtable collaborator permissions.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will VIU notify them of the update, correction or annotation?

The CIO or ITS manager assigned by the CIO can modify, update, or correct an individual's information at their request in the Airtable software. Individuals can also self-correct information in the employee portal or ask Human Resources to update or correct employee information that cannot be self-corrected in the portal. This updated information would be pulled from an HR database into Airtable or, if automation doesn't work, VIU ITS managers would periodically update the information manually.

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

Yes: the organizational chart could result in employees being moved to other areas or positions.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

It is in the proponent's best interests to keep personal information up-to-date, accurate, and complete. The information is also based on and drawn from Human Resource databases so the information will reflect the HR records.

19. If you answered "yes" to question 17, do you have approved records retention and 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?

[redacted] s. 15(1)(l); s. 17(1)

In addition, it is noted in the proponent responsibility section at the end of this PIA that the proponent must retain records for at least one year where personal information is used to make a decision that affects an individual.

Part 5 – Further Information

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

No.

21. Access for Research or Statistical Purposes: Will the information collected be used for research or statistical purposes?

Possibly for statistics internal to the ITS department, but not for wider distribution or publication, and not for research purposes.

Resources:

Air Table Privacy Policy

Airtable Privacy Whitepaper

Airtable Security Whitepaper

List of Airtable Subprocessors

Part 6 -- Summary and Proponent Responsibility

Privacy Office Comments:

The proponent intends to use Airtable software to build a dynamic organizational chart for departmental use. The use of Airtable web-based software will necessitate the transfer of personal employment information of VIU employees to the Airtable software platform that is based in the USA and stores information on servers located primarily in the USA, with customer support subprocessors based in other jurisdictions. In such circumstances, BC FIPPA requires a rigorous assessment of the company's privacy and cybersecurity practices. Based on the review of Airtable's Privacy and Security polices it is evident that the company adheres to high international standards for both cybersecurity and privacy. As such, the Privacy Office recommends that the proponent proceeds with the initiative as outlined provided the following conditions are met to ensure compliance with BC FIPPA:

- The proponent must only collect personal information elements that are necessary for the purpose of the initiative.
- Where personal information is used to make a decision that directly affects an individual, such as changing roles, job requirements, etc. the proponent must retain that personal information for at least one year after the decision (as per section 31 of FIPPA).
- The privacy office recommends that the proponent notify its employees of their intent to use Airtable and disclose the fact that the information will be stored on servers outside of Canada. The proponent should give employees an option to opt out. In such cases, the proponent would be limited to using name, position title, and business contact information.
- The proponent will only use the software for building the organizational chart. If the proponent decides to use Airtable for any activity that involves integration with other software, apps, or systems, they will contact the Privacy Office to add an addendum to this PIA.
- Should the proponent decide to go-ahead with Strengths Finder, they must contact the Privacy Office for an addendum or separate PIA if any additional personal information will be collected.
- If the proponent decides to ask for employees' dietary needs, they should inform them that they plan to put this information in Airtable.

Part 7 -- Signatures

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Role	Name	Electronic signature
Initiative lead	**Omair Quraishi** Chief Information Officer	[redacted]
Program/Department Manager (if different from initiative lead)		[redacted]
Privacy Officer / Privacy Office Representative	**Mike Culbertson** FOI & Privacy Officer	[redacted]

s.22(1)