SFU UNIVERSITY SECRETARIAT | ARCHIVES AND RECORDS MANAGEMENT DEPARTMENT

PRIVACY IMPACT ASSESSMENT (PIA)

for

ESRI ArcGIS Online

Table of Contents

Before you begin

This form is used by SFU to determine if a new or a proposed substantial change to a system, project, program or activity meets or will meet the protection of privacy requirements under Part 3 of the British Columbia *Freedom of Information and Protection of Privacy Act* (FIPPA). FIPPA makes it a legal requirement that SFU conduct a PIA in accordance with the directions of the minister responsible for the Act. The PIA is a risk management and compliance tool to identify potential privacy issues and impacts, allowing correction and mitigation, thus avoiding costly redesign; privacy complaints or breaches; and harm to personal, professional and institutional reputation.

Before you begin this form, please contact the Privacy and Access Program, through the Archives and Records Management Department. See more information about the process here: https://www.sfu.ca/archives/fippa/privacy-impact-assessments.html.

PART ONE, SECTION 1: GENERAL INFORMATION

PIA file number: 2022-009

Initiative title:	ESRI ArcGIS Online
SFU Department / Faculty:	Library
Branch or unit:	
Link to SFU initiative website:	https://www.lib.sfu.ca/find/other-materials/data-gis/gis/software
Link to vendor website:	https://www.arcgis.com/index.html
Link to vendor privacy policy:	https://trust.arcgis.com/en/privacy/privacy-tab-intro.htm, see also Esri DPA on their website.
Your name and title:	Mark Jordan, Associate Dean of Libraries
Your work phone and email:	778-782-5753 / mjordan@sfu.ca
Initiative Lead name and title:	Same as above
Initiative Lead phone and email:	Same as above
Privacy Rep	Erika Brimacombe, Privacy Legal Counsel
Privacy phone and email:	778-782-4042, erika_brimacombe@sfu.ca

A. Related PIAs, if any:

- None

B. If this initiative involves an external service provider or vendor, has a contract between SFU and the vendor been signed?

- License renewal due Dec 2022, renews every 3 years. The license covers desktop client and cloud-based products. Esri DPA applies.

C. Has SFU's "Privacy Protection Schedule" been agreed to by the vendor?

- No. Robust pre-signed DPA applies to all Esri contracts.

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

ArcGIS Online (AGOL) is a cloud-based mapping and analysis application by ESRI, enabling users to search for spatial data, create maps, web apps, analyse data, publish data and maps as data layers and web maps hosted on the cloud, share content, and collaborate with others. SFU Library negotiates an educational site license with ESRI which includes desktop client and AGOL. The usage has grown to nearly 1200 SFU users, including faculty members, staff and students. It is anticipated that the usage will continue to increase, perhaps quickly, particularly when we start to include AGOL on the Library's page about access to Esri ESRI applications (currently there is no mention of AGOL on the page).

The library currently assigns AGOL accounts to users manually upon receiving a user's request: setting up an account and then emailing the user to notify him/her along with a privacy notice, which was drafted based on the suggestions provided by Alexandra Wieland, the Information and Privacy Archivist at the time. This process is labour-intensive and error prone. In addition, graduated students will have to be manually removed from the users list, and thus creating extra workload for the library staff.

Given the above reasons, the library is seeking to implement an SAML Login (previously known as Enterprise Login) for AGOL, which will automate creating AGOL accounts for SFU community members, and hence significantly reduce the workload for the library staff in administering AGOL. With SAML Login, SFU users will be able to sign in with SFU ID. Upon verification of the member's credentials, SFU's identity provider informs AGOL of the verified identity for the member who is signing in and create an AGOL account.

There are a few other ESRI products that can be accessed using an AGOL account, including ArcGIS Pro and a suite of apps such as StoryMaps, FieldMaps, Business Analyst, and so on. Therefore the deployment of AGOL SAML Login will facilitate the use of these products. Those products do not collect different personal information (users log into their AGOL account to access the apps). The apps are included in the scope of this PIA for future use.

ArcGIS Pro is a desktop ESRI application included in our Education Site License; it gives users an option to connect to AGOL within the program. ArcGIS Pro has two licensing models -- single use license and named user license. The library currently provides single use license for ArcGIS Pro for the reason that it allows for offline use, giving end-users flexibility (for example, unstable internet connection). However, with single-use licensed ArcGIS Pro, users will still be able to log-in within ArcGIS Pro and connect to AGOL so that they can download data from AGOL or publish maps.

For class assignments, there are two scenarios: first, the instructor creates an AGOL group for a class of students, who collectively contribute data to a map. The students can't see other students' edits but the instructor can see all edits. This type of situation might be considered "administered assignments" on AGOL.

The second kind of situation is that students create their unshared work and once it's done they send the URL of the work to the instructor.

The profile setting on AGOL includes options of "private", "organization", and "public". In the collection notice, we include a note recommending that they set their profile to be private.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

SFU's use of AGOL, SFU-wide, including ArcGIS Pro and a suite of apps within AGOL such as StoryMaps, FieldMaps, Business Analyst, and so on

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix. Consider segmenting your response into the different categories of people who you will collect different types of information from (e.g. students, administrators, employees, alumni, etc.)

- Full name and SFU email address through single-sign-on, for account creation
- Unique user-created user-name and password
- Additional, optional profile information supplied by user
    - This includes an optional bio, an optional photo, and a field for other optional, undesignated information.
    - Visibility of the bio/profile defaults to be "organization", but can be changed to "private" or "public". Not sure if we can disable the bio – we may need to test it with the team who will set up the SSO. The SFU administrators of AGOL can see all the information users enter, even if set to "private".
    - SFU may or may not be able to disable this bio/profile option, and will look into this further.
- IP address through cookies (option to disable)
- Content created through ArcGIS (data, maps, etc.)

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference. For example:

- *names, home addresses, emails, and telephone numbers of the individual or of their guardians or family members;*
- *images of the individual;*
- *anyone else's opinions about an individual;*
- *an individual's personal views or opinions;*
- *identifying number (e.g., student number, employee number, health care number;*
- *age, sex, gender, marital status, race, national or ethnic origin;*
- *religious or political beliefs or associations;*
- *educational, medical, criminal, financial, employment history.*

Type "yes" or "no" to indicate your response.

Yes

- ***If yes**, are all of the personal information elements you are collecting necessary for your initiative?*
  - Yes, save for the option users have to add unnecessary profile personal information and photos, which SFU will request they do not do in the collection notice. SFU will also look into disabling this profile feature.
- ***If no,** how will SFU reduce the risk of unintentionally collecting personal information? After you answer this question, submit this PIA to the Access and Privacy Program. **You do not need to complete the rest of the PIA template**.*
  - N/A

SECTION 2: COLLECTION, USE AND DISCLOSURE

4. Collection, use and disclosure flow

Describe the information flow of your initiative in the below chart.

- **Collection**: *Describe the steps in collecting personal information from individuals by SFU and/or the vendor (be sure to clarify which party is collecting the information).*
- **Use**: *How does SFU and/or the vendor use the personal information collected (be sure to clarify which party is using the information)?*
- **Disclosure**: *When, if ever, would SFU and/or the vendor provide the personal information to a third party who does not normally have access to the personal information?*

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FIPPA authority** *See the most common FIPPA authorities listed below this chart.*	**Other legal authority**
Step 1: A student logs in to AGOL for the first time through SAML Login using his/her university credential and creates an AGOL account	Collection	26(c)	
Step 2: Students will have the option to complete their profile: some fields are pre-filled based on what was passed from the SAML configuration. Only username, first and last name are mandatory.	Collection	26(c)	
Step 3: AGOL account is used to provide user-generated content and information (data uploaded and web maps, hosted layers, web apps created by a user).	Use	32(a)	
Step 4: ESRI technical support staff may require personal information to identify system problems or to assist individual system users with specific problems and troubleshooting.	Use	32(a)	

Most Common FIPPA Authority References

For more options, see the full text of FIPPA (link).

Type	Description	Section
Collection	The collection of the information is expressly authorized under an Act	26(a) **and list the enactment and section above*
	The collected information relates directly to and is necessary for a program or activity of the University.	26(c)
	The collected information is necessary for the purposes of planning or evaluating a program or activity of the University.	26(e)

Type	Description	Section
Use	Use of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose.	32(a)
	The individual the information is about has consented to the use (*If using this authority, provide a copy of the consent language after your collection notice, below)*	32(b)
	Use of the information is for a purpose for which the information may be disclosed to the public body under FIPPA s. 33	32(c) **also list which authority under s.33*
Disclosure	The individual the information is about has consented to the disclosure (*If using this authority, provide a copy of the consent language after your collection notice, below).*	33(2)(c)
	Disclosure of the information is for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose. (*If you select this authority, ensure the disclosure is described in the collection notice, below).*	33(2)(d)
	Disclosure of the information is in accordance with an enactment of British Columbia or of Canada that authorizes or requires the disclosure: *[insert detail]*	33(2)(e) **and list the enactment and section*

***Optional**: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.*

5. Collection Notice and Consent

5.1 Collection Notice: *If you are collecting personal information directly from an individual the information is about, FIPPA requires that you provide a collection notice (except in limited circumstances). If your vendor is collecting personal information on behalf of SFU, the vendor must also provide a collection notice.*

Review the template collection notice and update as applicable. Consider whether you will need more than one collection notice.

This collection notice will be provide/shown to students at the Library's connection/access page for AGOL: https://databases.lib.sfu.ca/record/61245147670003610/ESRI-(Environmental-Systems-Research-Institute)-Software.

The information you provide through ESRI's ArcGIS Online is collected by SFU under the authority of the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c.165). The personal information collected by ArcGIS Online includes your name, email address, IP address, optional profile information you choose to include, and content you create within the program.

Please do not include optional sensitive personal information in your profile, and we recommend you set your profile settings to "private".

ESRI stores your personal information outside of Canada, in the United States. You may wish to review ESRI's privacy policy here: https://www.esri.com/en-us/privacy/overview. The information collected is used to provide you access to create content in ArcGIS Online, improve services, and unless you opt out, provide you with marketing materials. If you have any questions about the collection and use of this information please contact the Associate Dean of Libraries (Digital Strategy), libhelp@sfu.ca, (778) 782-4706.

5.2 Consent: *If you are obtaining consent for the use or disclosure of personal information, add any consent language here.*

Consent must have the following elements:

- *a) be in writing; and*
- *b) be done in a manner that specifies:*
  - *a. the personal information for which the individual is providing consent;*
  - *b. the date on which the consent is effective and, if applicable, the date on which the consent expires;*
  - *c. for "use" consent, the use of the personal information; and*
  - *d. for "disclosure" consent:*
    - *i. to whom the personal information may be disclosed;*
    - *ii. if practicable, the jurisdiction to which the personal information may be disclosed; and*
    - *iii. the purpose of the disclosure of the personal information.*

N/A

SECTION 3: STORING PERSONAL INFORMATION

6. Is any personal information stored outside of Canada?

Type "yes" or "no" to indicate your response.

Yes

- *If yes, where (e.g. which states or countries)?*
  - USA

7. Does your initiative involve sensitive personal information that will be stored outside of Canada?

"Sensitive" is not defined. What information is sensitive may depend on the context. Examples can include medical information, unique government issued identifiers (passport number, driver's license, PHN, SIN), financial information, disciplinary or complaint history, etc. You may need help from the Access and Privacy Program to determine whether the personal information is "sensitive".

Type "yes" or "no" to indicate your response.

No

- *If yes, go to question 8.*
- *If no, skip ahead to Section 5.*

8. Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public?

Type "yes" or "no" to indicate your response. "No" is the most likely response.

N/A

- *If yes, what enactment? Then skip Section 4 and go to Section 5.*
  - N/A
- *If no, go to Section 4.*

~~SECTION 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA~~

~~*Complete this section **only if** sensitive personal information will be stored outside of Canada.*~~

~~9. Storage details~~

~~*Fill in the table below (add more rows if necessary)*~~

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

10. Does the contract you rely on include privacy-related terms?

Type "yes" or "no" to indicate your response.

[Answer]

- *If yes, describe the contractual measures related to your initiative, or copy the terms in here.*
  - [Answer]
- *Has SFU's Cloud Privacy Protection Schedule been appended to the contract?*
  - [Answer]

11. What controls are in place to prevent unauthorized access to sensitive personal information?

[Answer]

12. Provide details about how SFU or the vendor will track access to sensitive personal information.

[Answer]

13. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.

Outcome of Section 4

The outcome of Section 4 will be **a risk-based decision made by the University's delegated authority on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17.

Is the outcome to proceed with the initiative? Type "yes" or "no" to indicate the response.

N/A

SECTION 5: ACCURACY, CORRECTION AND RETENTION

14. How will SFU and/or the vendor make sure that the personal information is accurate and complete?

FIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

The user is responsible for creating and managing their AGOL profile and information. AGOL does not pull or rely on outdated personal information.

15. Requests for correction

FIPPA gives an individual the right to request correction of errors or omissions to their personal information. SFU's formal process to respond to these requests is here: Requesting a Correction to Personal Information in University Records.

15.1 Do you or your vendor have a process in place to correct personal information?

Type "yes" or "no" to indicate your response.

Esri will permit users to access, correct, or delete their information in the database by contacting info@esri.com or by logging in to their user account and making the appropriate changes. Esri's privacy policy states it will respond to all requests for access within a reasonable timeframe.

15.2 Sometimes it's not possible to correct the personal information. FIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you and your vendor document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

Yes

15.3 If you and/or the vendor receives a request for correction from an individual and you know you disclosed their personal information in the last year to one or more third parties, FIPPA requires you to notify the parties you disclosed to of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

Yes – but the circumstances of this being required are not foreseen at this time.

16. Does your initiative use personal information to make decisions that directly affect an individual?

Type "yes" or "no" to indicate your response.

No.

- If yes, go to question 17
- If no, skip ahead to Section 6

17. Do you have an records retention schedule in place related to personal information used to make a decision?

FIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Type "yes" or "no" to indicate your response.

N/A

- *If no, describe how you and/or the vendor will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.*
    - The ESRI privacy policy states "We will retain the personal information we process on behalf of our users for as long as needed to provide services to our users, comply with our legal obligations, resolve disputes, and enforce our agreements."

SECTION 6: ADDITIONAL RISKS

18. Has the vendor expressed, either through contract, communications with you, or their privacy policy, their agreement to notify SFU of a privacy breach?

Under s.30.5 of FIPPA, an SFU employee or service provider to SFU "who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the [University Archivist and Coordinator of Information and Privacy]".

Privacy breaches can be reported to SFU here:
https://www.sfu.ca/archives/fippa/breaches-complaints/report-respond-to-a-breach.html

Yes. See Esri Data Processing Addendum which applies to agreements with customers.

19. Risk Response (non-security risks)

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Proportionate Response / Mitigation Strategy
[redacted]	

SECTION 7: PRIVACY SIGNATURE

This PIA was conducted by the Delegated Authority below, in accordance with the Minister of Citizens' Services Direction 2-21 and SFU Policy I 10.02 'Head of the Institution and Delegation of Authority under FIPPA'.

Role	Name & title	Signature	Date signed
Privacy program representative (Delegated Authority)	Erika Brimacombe, Privacy Legal Counsel		May 18, 2022

20. Is the Delegated Authority's signature contingent upon review and signature by Information Security per Section 2?

If yes, provide PIA to Information Security to complete Section 2, below.

Yes

21. Privacy Recommendations:

[redacted]

PART 2: SECURITY OF PERSONAL INFORMATION

For Review by SFU's Information Security

In this Part, you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

1. Cloud Security Protection Schedule

Has the vendor agreed to or signed a Security Protection Schedule?

N/A

2. Vendor's Physical and Technical Security Arrangements

Vendor's Security Arrangements: *If this initiative involves a vendor, what are their physical and technical security arrangements for protecting the personal information in their custody against such risks as unauthorized collection, use, disclosure, or storage?*

See: https://trust.arcgis.com/en/security/security-overview.htm

See also Esri DPA: https://www.esri.com/content/dam/esrisites/en-us/media/legal/gdpr-data-processing-addendums/data-process-addend.pdf (image from DPA copied below).

[redacted]

3. Controlling and tracking access

Please check each strategy that describes how you or your vendor limits or restricts who can access personal information and how you keep track of who has accessed personal information in the past. Insert additional strategies if needed.

Strategy	Yes/No
[redacted]	

Strategy	Yes/No
[redacted]	

4. Risk Response (Security Risks)

Describe any security risks that arise in your initiative that have not been addressed by the questions on the template. Add new rows if necessary.

Possible risk	Proportionate Response / Mitigation Strategies
[redacted]	

5. Information Security Comments and Signature

5.1. Does this initiative have reasonable security arrangements?

- Yes

5.2 Comments / Recommendations:

-

Role	Name & title	Signature	Date signed
Information Security representative	Steve MacGregor, CIPT, PCI ISA Information Compliance Architect		2022-06-01

PART 3: ACCOUNTABILITY

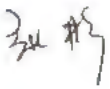
The Minister of Citizens' Services Direction 2-21, "Privacy Impact Assessment Directions" requires that all PIAs "Designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s.D8).

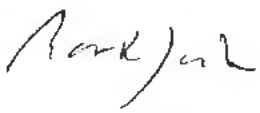
The accountability is maintained by the role or position, regardless of who fills the role. The role responsible for deciding whether or not to implement the initiative referred to in this PIA is the role most likely to be appropriate for holding accountability.

Under SFU's Protection of Privacy Policy I 10.11, Administrators are responsible for:

- *Ensuring that the activities of their departments are in compliance with the privacy principles articulated in the Policy;*
- *Preparing Privacy Impact Assessments; and*
- *Abiding by the requirements of a completed Privacy Impact Assessment, including taking steps to correct or mitigate any privacy issues or foregoing the implementation of an initiative if the implementation is in violation of FIPPA or SFU policies.*

Accountability includes affirming that this PIA accurately documents the data elements and information flow at the time of signing.

Role	Name & title	Signature	Date signed
Initiative lead	Sarah Zhang, GIS Librarian		June 1, 2022

Role	Name & title	Signature	Date signed
Role designated accountable for the initiative	Mark Jordan, Associate Dean of Libraries – Digital		June 1, 2022

Schedule A

Types of security measures	
Physical	1. SFU data centre and backup data centre are both located on SFU campuses in Canada 2. Locked doors 3. Key card and electronic access control devices 4. Securely stored computing equipment 5. Receptionist supervision 6. Physical barrier to the public 7. Staff only access 8. Alarm systems 9. After hours security patrol checks
Technical	1. Firewalls 2. Encrypted network transmission 3. Tiered network infrastructure 4. Identity assurance provided by SFU's main Systems of Record 5. Role-based user access assigned on a need-to-know basis 6. Log-on user ID and password (single sign-on) provided by SFU's Central Authentication Service (CAS) 7. Timed out computer sessions
Security Policy, Procedure and Standards	1. University Policies e.g., GP-24 Fair Use of Information Systems, I 10.04 Access to Information and Protection of Privacy, I 10.05 Collection of Personal Information, I 10.09 Retention and Disposal of Student Exams or Assignments, and I 10.10 Confidentiality Policy 2. Designation and authentication of authorized users is managed through SFU's Identity and Access Management (IDAM) infrastructure, which is registered with the Canadian Access Federation (CAF) 3. SFU's IDAM infrastructure is benchmarked against the InCommon assurance program (http://incommn.org), which certifies campuses, non-profits and research organizations to determine the accuracy of a user's electronic identity and help mitigate risk for the service provider. While InCommon certification is not available outside the US, the assurance program serves as a benchmark for international standards and best practices 4. SFU's Privacy Protection Schedule is included as part of a signed agreement with a service provider of digital storage when purchased through Procurement, which includes provisions relating to data ownership, use, disclosure, security, retention and confidential/permanent deletion

	5. SFU has signed an Information Sharing Agreement with the public body describing the terms and conditions of their data-linking initiative or common or integrated program or activity 6. Authorized users of the IT system are made aware of protection of privacy rights and responsibilities by means of notices when logging onto the system; education by through the SFU website, workshops and advisory service; and/or signing SFU's Privacy and Confidentiality Agreement 7. Personal information is retained and disposed of according to an existing Records Retention Schedule and Disposal Authority approved by the University Archivist
Tracking Access / Access Controls	1. IDAM infrastructure assures identity 2. Role-based access management infrastructure authorizes access 3. Auditable log files