

Procurement of Software as a Service (SaaS) Solutions

Unlike on-premise software solutions, SaaS solutions are typically hosted in cloud data centres such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud. Given that SaaS solutions typically involve storing student or employee data in the cloud, we need to take very specific steps to ensure that your SaaS solution is secure and compliant with applicable privacy laws.

UVic [Purchasing Policy FM5105](#) requires that academic or administrative units obtain technical approval from University Systems in conjunction with the procurement of IT Devices and Services. This page describes the typical considerations and process for acquiring Software as a Service (SaaS) solutions, with the goal of streamlining the process for obtaining technical approval.

Special Considerations

In addition to your functional requirements, we strongly recommend you consider the following elements in your requirements gathering and decision making process:

- **Privacy** – as a public body in British Columbia, we are bound by the requirement of the BC Freedom of Information and Protection of Privacy Act (FIPPA) to ensure that data at rest remains within Canada, especially if student data is involved. As such, the question of data residency should be one of the first enquiries to potential vendors. There are some potential workarounds if Canadian data residency is not available, however it is much more cumbersome and may restrict how the system and data can be used.
- **Security** – we are also bound by FIPPA and University Policies to ensure the privacy and security of personal data in our custody. Because SaaS solutions store data in the cloud, we need to ensure that vendors have appropriate security measures in place. Ideally SaaS vendors will have SOC 1 & 2 and ISO 27001 / 27018 security certifications for the entire software platform with annual third party compliance audits that are available to UVic. This should be the second question posed to vendors following Canadian data residency.
- **Accessibility** – with so many activities taking place online, it is important that all users are able to leverage adaptive technologies (e.g. screen readers) if required. Therefore it is important to ask about compliance with Web Content Accessibility Guidelines (WCAG 2.1) for all features, especially for student-facing applications.
- **Single Sign-on (SSO)** – it is helpful for students and employees to be able to log into SaaS services with their UVic Netlink ID and password, rather than using separate usernames and passwords. This is particularly important because people tend to use the same usernames and passwords in multiple services, which potentially creates vulnerabilities at UVic if just SaaS is compromised. As such we recommend asking the vendor if they support CAS and SAML single sign-on (SSO) to enable the use of UVic logon credentials.

Procurement Process

UVic Purchasing Services is responsible for ensuring that all procurements at UVic are compliant with applicable legislation and trade agreements. The Purchasing website offers lots of general guidance on [purchasing goods and services](#) and the [phases of procurement](#)., which are also applicable to SaaS solutions.

The SaaS procurement and software lifecycle typically involves the following components, with higher valued procurements simply undergoing a more rigorous process with more defined steps.

1. **Opportunity** – assess options and risks, estimate investment, and develop a high-level strategy with broad stakeholder support for moving forward
2. **Requirements Gathering** – gather sufficient functional and technical requirements
3. **Decision Making** – select a vendor to initiate negotiations with
4. **Privacy/Security Assessment** – ensure vendor platform complies with BC privacy legislation (FIPPA) and industry-standard security requirements (e.g. ISO)
5. **Contract Negotiation** – establish mutually agreeable contract terms
6. **Contract Execution** – both parties sign mutually agreed contract
7. **Implementation** – configure the system, load data, train and onboard users
8. **Sustainment** - leverage the system to meet your functional needs and ensure that the system remains functionally and technically current

The value of the solution drives the overall procurement approach.

- **Under \$15,000** - identify and select a vendor of your choice to begin contract negotiations
- **Between \$15,000--\$75,000** – collect quotes from three different vendors before deciding between them, or work with Purchasing Services to run a competitive selection process
- **Over \$75,000** – work with Purchasing Services to run a competitive selection process

In most cases a SaaS contract consists of the following elements:

1. **Vendor Terms and Conditions** – UVic may request amendments
2. **UVic Privacy Protection Schedule** – Vendor may request amendments
3. **UVic Cloud Security Schedules** – Vendor may request amendments

Once you have these contract elements the general process is to:

1. Document the following information about the system:
 - a. Who will use the system and for what purpose (e.g. general use case)
 - b. What kinds of data will be stored (e.g. name, email address, application data)
 - c. Whether data at rest remains inside Canada – vendor can provide this information
 - d. Whether the vendor has any security certifications with third-party attestation for the entire software platform (e.g. SOC, ISO) – vendor can provide this information
2. Review contract elements above with Purchasing Services, vendor, UVic General Counsel and Chief Privacy Officer, and University Systems
3. Attach the above information, including mutually agreed Terms and Conditions, UVic Privacy Protection and Cloud Security Schedules to WebReq for Technical Review by University Systems and contract execution by Purchasing Services.