Published on *University of Colorado* (https://www.cu.edu)

Security Guidance for Software as a Service [1]

Introduction

This guide is for departments and teams who are considering Software as a Service (SaaS) options for their technology needs. These options place much of the technology management in the hands of a third-party, which can be efficient and effective, and also means teams have to be diligent in understanding the effect on information security.

SaaS Information Security Considerations

A SaaS product used for the University of Colorado community should strive to meet the following requirements. While we recognize that different use cases may require more or less stringent guidelines than those outlined here, the checklist has been designed to be a good starting point for any purchaser of a Software as a Service product.

Does the product meet applicable information security standards and compliance requirements?

- CU has differing levels of information security standards based on the risk level of the service, including the sensitivity of the data it handles. Contact your information security team for guidance.
- Reputable SaaS providers document their alignment with relevant compliance standards/processes. This is often demonstrated by conducting a third-party audit that is documented in a report like a SOC 2 Type II. Potential customers can request a copy of these reports to review.
- Some forms of business have specific regulatory or contractual requirements. If this applies, there might be other documentation to request. For example, payment card processing services should be able to demonstrate compliance with the Payment Card Industry Data Security Standard (PCI-DSS), and services that handle patient data may need to be compliant with the Healthcare Insurance Portability and Accountability Act (HIPAA).

Has an information security review been performed?

- IT procurements require a security review to assist with assessing risk, validating security requirements and ensuring appropriate contract language is used.
- Processes vary by campus and the security review may be combined with reviews for accessibility or other requirements.
- Contact your campus information security team for details.

How will CU data be handled across the lifecycle of the product?

- Using a SaaS service often requires copying some amount of CU data into the service. This data must be handled properly for functionality, security and privacy.
- Verify whether CU data is encrypted in transit and at rest when it is handled by a third-party.
- CU should retain ownership of its data and the third-party should only be permitted to use CU data to provide services to CU. This is typically managed by wording in the contract with the third-party.
- Establish an expectation with the third-party about how CU data will be handled once the agreement reaches its end. This could mean that CU has the ability to export all of its data and that the third-party will delete all CU data after a certain period of time. Be sure to include these requirements in the written agreement with the third-party.

How will users log into the service and how will their access to functions and data be managed?

- There are many ways to log into a third-party IT service, and it's important to verify that the available options are compatible with campus login services. Luckily, there are well-established standards (e.g., SAML, OAuth, OIDC) that make this easier. Verify that the product supports a login mechanism that is supported by your IT department.
- Managing access and roles within a service can vary greatly between products. Some products offer the ability to use existing groups or attributes to grant access. Some require manually creating roles and assigning access. Consider your needs for managing access to verify that the product can meet those needs.

How can the service be monitored for possible security incidents? If a potential incident is discovered, does the service have good capabilities for allowing security teams to investigate the issue?

- There are multiple ways a service could help raise alerts of possible security incidents. Verify what options are available and how to ensure the alerts are promptly communicated. Examples include:
    - Built-in email alerts for suspicious events.
    - Logs sent to a security log server for automated monitoring.
- Once you've been alerted to a possible security incident, your information security team will likely want to investigate. Here are some examples of features that would make that process easier:
    - Easy access to detailed logs about what is happening in the service.
    - Access to 24x7 support from the service in case of off-hours security issues.
    - Proactive notifications from the service via email, blog, text, etc.

For more information, contact your campus IT or information security team.

Updated August 27, 2024

Groups audience:
Office of Information Security
Right Sidebar:
Information Security Campus Contact
IT Departments Campus Contact

Links
[1] https://www.cu.edu/security/security-guidance-software-service