

TECHNOLOGY VENDOR RISK ASSESSMENT

Section:	Administration (AD)
Subject:	Institute and Non-Institute Services
Legislation:	<i>Freedom of Information and Protection of Privacy Act (RSA 2000 c.F-25); Health Information Act (RSA 2000 c.H-5).</i>
Effective:	November 24, 2021
Revision:	

APPROVED: _____
President and CEO

POLICY

The policy of the Board of Governors is to ensure that SAIT's information and related technology assets and service are managed effectively through a control framework.

PHILOSOPHY

The outsourcing of information technology services allows SAIT to take advantage of economies of scale, greater efficiency, greater quality, greater security and greater compliance. However, it also creates risks for SAIT if the use of the technology and the information security posture of the service and vendor are not carefully evaluated.

This evaluation reduces risk and provides for the confidentiality, integrity, availability and privacy of all members of the SAIT community as well as for the Information Technology Systems department. It establishes fundamental security guidelines, requirements and procedures that support the mandatory protection of information assets for business, contractual, regulatory and legal purposes.

DEFINITIONS

Employee A person employed on SAIT's payroll, whether paid by annual salary or hourly wage, and contractors.

The official controlled version of this document is held in the Board of Governors Office.



Institutional data

Data that is created, collected, maintained, transmitted and stored by or for the institution to conduct institution business. It includes data used for planning, managing, operating, controlling or auditing institution functions and operations and as defined by the Data Governance Council/Steering Committee. It is not limited to data or information stored on centrally managed databases/servers. Data can also be stored on hosted services, individual desktops, paper files and electronic files such as spreadsheets.

GOVERNING PRINCIPLES

1. This procedure applies to all SAIT systems and assets, employees, vendors and agents operating on behalf of the institution.
2. Outsourced IT services that are used to store, process, or transmit data shall be subject to review regardless of cost.
3. Individual schools/departments may choose to have additional security and controls that are greater than those outlined in this procedure.

PROCEDURE

1. If the vendor or service will access institutional data, the acquisition process will include a third-party risk assessment completed by the vendor. The requesting school/department ("requestor") will require the vendor to complete the third-party risk assessment as soon as they decide to engage the vendor for the solution.
2. The Request for Proposal ("RFP") process requires the vendor finalists to complete the third-party risk assessment. The results of the information contained within the third-party risk assessment should be taken into consideration when choosing a vendor using the RFP process.
3. Completed third-party risk assessments will be reviewed by the Information and Technology Services' department's Information Security team. If additional questions arise as the result of the completed assessment, Information Security team employees will reach out to either the requestor or vendor contact, depending upon the nature of those questions. It may take longer to obtain approval for technology solutions that access sensitive or restricted data than for solutions that do not access such data.

The official controlled version of this document is held in the Board of Governors Office.



4. Upon approval of a vendor/solution, the requestor will be notified via email or an approval message through the Procurement department.
5. The requestor should be aware that certain types of data require SAIT to comply with external mandates for protected information compliance. Such mandates include but are not limited to:
 - a) *Alberta's Freedom of Information and Protection of Privacy Act*, specifically in relation to student records.
 - b) *Alberta's Health Information Act*: contracts involving the third-party handling of protected health information require a Privacy Impact Assessment with the third party.
 - c) Payment Card Industry Data Security Standards (PCI-DSS): contracts involving the processing of credit card payments and related services within the scope of PCI-DSS must include PCI compliance contract language.
6. Periodic review of a vendor's security posture and continued compliance will be conducted as needed, based upon changes in system use, design or controls, contract renewal or business transfer, merger, or acquisition.

POLICY/PROCEDURE REFERENCE

- AD.2.10 Information and Technology Management policy
- AD.2.10.1 Password Protection procedure

The official controlled version of this document is held in the Board of Governors Office.