FN.7.1.3 Procurement Procedure

Schedule C - Technology Acquisition and Procurement Process

PHILOSOPHY

All technology-related procurement decisions, including those involving third-party services, software and/or infrastructure, must be thoroughly evaluated to ensure alignment with SAIT's institutional priorities, risk management policies and privacy and security standards.

DEFINITIONS

Application development	The process of designing, building, testing and deploying software applications to meet specific user requirements or resolve business challenges. This process involves coding, system integration and continuous enhancements to functionalities across web, mobile and/or desktop platforms.
Cloud computing services	Delivery model where software applications or services are hosted by a cloud computing service provider and accessible to users via the internet. This approach enables organizations to use software on a subscription basis without managing the underlying infrastructure or installations. Cloud computing can include Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS).
Employee	A person employed on SAIT's payroll, whether paid by annual salary or hourly wage and contractors.
End-of-life	The stage at which a hardware or software product is no longer supported by the manufacturer or vendor. At this point, the product no longer receives updates, security patches and/or technical support, which may pose security risks or compliance issues for continued use.
Hardware	The physical components of a computer system or network, such as servers, computers, routers, storage devices and peripheral devices. These components form the foundational infrastructure that support and enable software applications and data processing.

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 Operating 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, devices, paper files and electronic files such as spreadsheets.
Non-supported software	Refers to software that is not institutionally supported, for which technical support may be provided by Information Technology Services (ITS), vendor support or by special agreement.
Shadow IT	Refers to the use of any unauthorized or unmanaged technology systems, applications or services within SAIT, typically without the knowledge or approval of ITS. Such practices may pose security, compliance and data management risks due to the lack of appropriate oversight. Shadow AI is a subset of Shadow IT involving AI tools or services used without review, potentially creating security, privacy or compliance risks.
Supported software	Refers to applications or systems that are officially maintained by the vendor or ITS, including receiving regular updates, security patches and technical support. Using supported software helps ensure reliability, compatibility and protection against known vulnerabilities.
Total Cost of Ownership (TCO)	The total cost associated with acquisition, deployment and/or transition, operation, maintenance of a product or system throughout its entire lifecycle and its retirement. This encompasses direct costs (such as purchase price and implementation expenses) as well as indirect costs (such as support, training, service and eventual replacement or disposal).

GOVERNING PRINCIPLES

1. The guidelines outlined in this process apply to all technology-related goods and services purchased or acquired on behalf of the institution, regardless of the funding source (including, but not limited to, school or department operating funds, Information Technology Services (ITS) central funds, grants, restricted funds, endowments or gifts). Technology purchased by or on behalf of an individual employee using academic employee professional development funding,

provided in alignment with the SAIT SAFA Collective Agreement, must comply with procedure HR.2.2.2 Professional Development Fund - Academic Employees.

2. Schools and departments engaged in detailed planning related to technology (such as workspace re-allocation and/or budget planning) must proactively engage ITS in the planning process. This includes sourcing vendor products that are either on-premises technologies (hardware, applications and non-supported and/or supported software) and/or cloud-based services and solutions.

3. Prior to procuring, acquiring or developing any technology solution, SAIT will require mandatory oversight from key departments and individuals, including but not limited to, ITS, Finance, Accessibility Services and from the Access and Privacy Unit, Office of General Counsel, as applicable. This oversight is required to ensure that SAIT receives the maximum benefit, in terms of cost and functionality, when purchasing IT equipment and/or technology services including, but not limited to:

    a) Hardware (e.g., computers, servers, networking equipment and mobile devices);

    b) Software (licensed or custom-built) or online services;

    c) Cloud computing and/or Connectivity from service providers;

    d) Technology services and/or consulting engagements.

4. Schools and departments must work with the ITS department and take into account the following key considerations during technology-related planning, application development, procurement, acquisition and/or decision-making processes:

    a) Strategic alignment and value: Technology must support SAIT's academic, research and administrative priorities, align with institutional strategies and digital transformation initiatives and demonstrate value through innovation, cost-effectiveness and licensing optimization;

    b) Total cost of ownership (TCO) and lifecycle management: Procurement decisions should consider the full lifecycle costs of technology (acquisition, licensing, training, maintenance, support, upgrades and decommissioning/disposal), with lifecycle and end-of-life planning built into sourcing;

    c) Security, privacy and risk management: All technology-related equipment and services must meet institutional, legal and regulatory standards for cybersecurity and data privacy and undergo appropriate risk assessments, including vendor security reviews, financial viability checks and completion of required Privacy Impact Assessments, as applicable;

d) Supportability, standardization and interoperability: Only technology that can be maintained and integrated by ITS should be approved and/or implemented. Preference should be given to solutions that align with institutional technology standards, promote interoperability and avoid duplication;

e) Cloud computing governance: All cloud-based solutions must follow SAIT's cloud and data guidelines/governance (such as data residency, service level agreements (SLAs) and exit strategies); and

f) Procurement through approved channels: Technology purchases must follow institutional procurement procedures, including obtaining proper approvals, engaging in competitive sourcing as required and purchasing through SAIT Preferred Suppliers, contracted suppliers and/or other approved methods of purchase, as outlined in procedure FN.7.1.3 Procurement.

5. Technology acquired or purchased outside of this process (e.g., Shadow IT) exposes the institution and the employee to risk and is strictly prohibited.

PROCEDURE

1. Schools/departments must follow the established purchasing processes, as determined by the Supply Management section of Finance and as outlined in FN.7.1.3 Procurement procedure, including utilization of SAIT Preferred Suppliers, when those suppliers are able to meet SAIT's purchase needs and requirements.

2. Employees engaged in the acquisition of technology-related goods and/or services must contact their designated purchasing officer in the Supply Management section of Finance, early in the acquisition process for technology requests, to accommodate the necessary timing for any required assessments and/or approvals, dependent upon the type of purchase and/or the technology, equipment or services that is being requested.

3. Supply Management will confirm with the requestor that the following individuals and/or departments have reviewed and provided support prior to procurement, as necessary:

   a) ITS for technical alignment and compatibility, support feasibility, cybersecurity, risk assessment and, if required, accessibility review with Accessibility Services;

   b) Finance for budget compliance and/or comparative price quotes; and

   c) Access and Privacy Unit for privacy review and privacy impact assessments, if required.

4. If the supplier product or service will access, process, manage or possess personal information or institutional data, the acquisition and/or procurement process will include a third-party risk and/or privacy assessment, in compliance with procedures AD.2.10.2 Technology Vendor Risk Assessment and AD.1.1.2 Privacy Impact Assessment (under development). Third-Party Risk and Privacy Assessment Requests must be submitted through ServiceNow and must include all supporting documentation.

5. When sourcing technology systems that will be purchased using grant funding or that are under contractual obligations to use specific equipment, ITS can assist the requesting area (i.e. SAIT researchers) in their computer equipment selection, to ensure that researchers are acquiring equipment that is suitable for their needs and that:

    a) Meets the risk management, privacy and security requirements of SAIT; and

    b) Meets the technology acquisition guidelines outlined in this procedure prior to being purchased/procured, connected, installed or utilizing institutional data.

6. Acquisition of SAIT supported mobile devices is facilitated through Commercial Services, to ensure proper device onboarding to SAIT systems and contract management. Devices purchased personally, with or without the use of professional development funds, are considered to be BYOD (bring your own device) and will only receive limited and basic SAIT ITS support, such as assistance with email and logins using SAIT credentials, access to campus wireless and print networks and/or VPN connections.

7. SAIT academic employees who purchase or intend to purchase hardware and/or software for professional development purposes must also comply with procedure HR.2.2.2 Professional Development Fund – Academic Employees.

8. Standardized computing hardware (such as SAIT laptops or desktop computers) can only be acquired via the ITS Service Desk submission form. Request or return a computer/laptop. Technology refresh of any additional devices that have been purchased by departments are not eligible for central ITS funding.

9. Any replaced equipment must be returned to ITS for repurpose, donation, recycling or disposal. Software and technology services will be subject to lifecycle reviews, as determined by ITS to ensure they remain current, updated and relevant to support institutional outcomes and objectives.

10. An employee who fails to comply with this process may be subject to discipline under procedure HR.4.4.1 Corrective and Disciplinary Action. Non-compliance may result in the removal of unauthorized technology and/or the cancellation of technology services.