Information Technology - Third Party - Security Policy

Section 1 - Purpose and Scope

Purpose

(1) Before procuring or implementing any third-party Information Technology (IT) services, a formal information classification and risk assessment must be undertaken by Technology Services. The risk assessment must be approved by the Director, Cyber Security, or Vice President (Operations) where there is high to significant risk. Third-party services not meeting minimum standards or lacking approval may be removed or isolated from the University's IT environment.

Scope

(2) Third-party IT services refer to IT services where the application and/or data reside on hardware not owned by the University. There are three main types of third-party IT services: hosting, software as a service (SaaS), and third-party computing.

a. In a hosting scenario, IT resources are allocated exclusively by the provider to the University, with minimal or no sharing of capabilities or costs among multiple user organisations.
b. In the third-party/cloud computing scenario, IT resources are allocated to applications and/or user organisations with elasticity, providing just-in-time, on-demand, and metered quantity and quality (advanced capability).
c. In the software as a service (SaaS) scenario, IT resources are offered to multiple user organisations using the same application, but each user organisation experiences it as if it were the only entity using the application.

(3) Non-SCU entities that operate IT resources or handle institutional information are considered third-parties for the purposes of this policy.

Section 2 - Policy

Risk Assessment

(4) Before procuring or implementing a third-party IT service, the Technology Services Cyber Resilience Team must conduct a detailed risk assessment. This assessment should identify risks associated with the implementation of the service, and an evaluation of these risks, along with appropriate management actions and mitigations, must be included in any business case.

(5) Throughout the lifespan of the third-party IT service, risks related to its ongoing use must be incorporated into the risk management plans of Technology Services and the business owners for periodic review. These plans should include specific risks related to upgrades, additions, and new versions of the system (whether initiated by the University or the vendor), as well as monitoring assurance reports provided by vendors.

Status and Details

Status	Current
Effective Date	3rd October 2024
Review Date	3rd October 2027
Approval Authority	Vice-Chancellor
Approval Date	2nd October 2024
Expiry Date	Not Applicable
Responsible Executive	Jack Williamson Vice President (Strategy & Technology)
Head of Work Unit	Jack Williamson Vice President (Strategy & Technology)
Enquiries Contact	Darron Richardson Director, Cyber Security Vice President (Strategy & Technology) Portfolio