Decision Framework on the Use of Cloud Services

This document is designed to provide the Curtin University community with a decision framework to help identify and understand the risks associated with cloud computing. However, this document is not intended to replace a comprehensive risk management process needed for deployment of a University-based cloud service.

Any systems, information or data hosted in the cloud that contains Personal and/or Sensitive Information is considered to be high-risk.

Below is a guide for the acceptable use of cloud services based on Curtin's Information Security Classification Policy and Procedures.

Cloud Services Use Inherent Risk Matrix

		Information Security Classification			
		Public	Internal Only	In-Confidence	Protected
Cloud System	Cloud services procured by the University using a formal project management approach, in consultation with Records & Information Management (RIM), Legal team, Risk Department and the Curtin Information Security Advisory Services.	Acceptable	Acceptable	Caution	Caution
	Public cloud services where the **data** is wholly l**ocated** in **Australia** and support is provided wholly within Australia. e.g. Telstra Cloud, Amazon Australia, iVec, Nectar	Acceptable	Acceptable	Caution	Caution
	Public cloud services where **data** is wholly located **outside of Australia** or support is provided with resources from outside of Australia.	Acceptable	Caution	Not acceptable	Not Acceptable

Where a proposed use of cloud computing is in the **red** section, contact RIM or the Curtin Information Security Advisory Services for information on additional encryption strategies *(e.g. Boxcryptor or Viivo)* to minimise or mitigate the information risks.

Where a proposed use of cloud computing is in the **yellow** section, the following issues/questions should be considered:

1. Legislative or contractual compliance
   a. Does the cloud provider meet contractual or legislative obligations to protect or manage the data/information, e.g. *Privacy Act 1988*, *Defence Trade Controls Act 2012*, *Freedom of Information Act 1992 (WA),* etc.? *(See policies.curtin.edu.au/compliance-and-integrity/ for more information)*
2. Data Ownership
   a. Does Curtin retain legal ownership of the data or information?
   b. Does Curtin have the right to access, audit, control, and delete data or information held in the cloud?
   c. Does Curtin have any control over subcontracting by the cloud service provider?
3. Data breaches
   a. Can the provider protect data/information against unwelcome adverse access or retrieval by parties other than Curtin and authorised agents?
   b. Will the provider notify Curtin of security incidents that mayor has affected Curtin data?
4. Data Integrity and availability
   a. Does the provider have mechanisms in place which prevents corruption or loss of data and guarantee both the integrity and availability of data/information?
   b. Can the provider quickly restore deleted data or information?

5. Public exposure
    a. What are the consequences if the data/information becomes publicly available?
6. Failure of provider
    a. What are the consequences if the provider fails to deliver the service?
7. Curtin's risk appetite
    a. Will the consequence be within Curtin's risk appetite? (please see Curtin's Risk Reference Tables)

Please contact RIM or Curtin Information Security Advisory Team if you require any assistance in considering the above questions. See also the Typical Risks on Using Public Cloud Services and Frequently Asked Questions regarding Cloud computing for more information.

Definitions:

Information Security Classification - A process where the creator of University Information assesses the sensitivity and importance of the information and assigns a label to the information so that it can be managed or stored with consideration to its sensitivity and importance.

Information Security Classification	Definition	Example
Public	Information that is publicly available and unlikely to cause harm to the University, another organisation, or an individual.	Prospective students course outlines, academic calendar, MOOCs resources and all information made available through Curtin's public website and social media sites
Internal Only	University Information that is generally not publicly available. The release of this information to the general public could cause minor harm to the University, another organisation, or an individual.	Academic lecture notes, third-party owned learning materials (subject to Copyright Act), policies, procedures, guidelines, etc.
In Confidence	University Information that must be kept confidential, access is on a need to know basis only. Unauthorised disclosure, modification, or destruction could reasonability be expected to cause harm to the University, another organisation or an individual; and provide an unfair advantage to an entity; or violate somebody's right to privacy.	Student academic records, student scholarship agreements, workers compensation, medical records, trademark certificates, deeds of settlements/release/discharge, Office of Research and Development contracts and agreements, tender documents, all security-related information such as encryption keys or password documents, etc.
Protected	Information that must be kept strictly confidential, access to the information must be restricted to only persons who are explicitly granted access to that information. Unauthorised disclosure, modification, or destruction could reasonably be expected to cause: • Serious harm to the University, another organisation or an individual; • Compromise Australia's national security; • Damage Australia's national interests, economy, stability or integrity; or • Damage Australia's international relations or defence.	Information which is subject to Defence Trade Controls Act 2012, information or documents for the University Council & Committees, research information requiring ethics clearances, information relating to allegations of fraud and professional misconduct.