Cloud Computing Use Inherent Risk Schedule

1 Purpose

To provide the University community with a decision framework to help identify and understand the risks associated with Cloud Computing.

2 Scope

This schedule must be read in conjunction with the Engagement of Cloud Services Procedure and is subordinate to it.

This document is not intended to replace a comprehensive risk management process needed for deployment of a University-based Cloud Computing service.

3 Schedule

3.1 Cloud Computing Use Inherent Risk Matrix

Below is a Cloud Computing Use Inherent use Matrix based on the Information Asset and Security Classification Procedure.

		Information Security Classification		
		Public Information	**Internal Information**	**Restricted Information**
Cloud System Category	Cloud Services procured by the University using a formal project management approach, in consultation with ICT Services, and consideration of the relevant legislation and University policies (e.g. QCIF eResearch Services, Office 365, Blackboard)	**Acceptable**	**Acceptable**	**Acceptable**
	Established and widely used public Cloud Services - Data centre is located in Australia, EU countries, Canada Hong Kong, Malaysia, South Korea, New Zealand (eg. Telstra Cloud, Amazon Australia)	**Acceptable**	**Acceptable**	**Caution**

	Established and widely used public Cloud Services - Data centre is located in the USA, China, Japan, India, Singapore, Philippines and Vanuatu (e.g. Dropbox, Google Docs, iCloud)	**Acceptable**	**Caution**	**Not Acceptable**
	Emerging Cloud Computing providers	**Caution**	**Not Acceptable**	**Not Acceptable**

Table 1: Cloud Computing Use Inherent Risk Matrix

Where a proposed use of Cloud Computing is in the red section, contact the Manager (Enterprise Information Management Services) or ICT Services for information on possible solutions or options.

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. *Information Privacy Act 2009*, *Right to Information Act 2009*, *Public Records Act 2002*, *Defence Trade Controls Act 2012*, *Crime and Corruption Act 2001?*

2. Data breaches
    a. Has the provider given a sufficient commitment to data security?

    b. Can the provider protect data/information against unwelcome adverse access or retrieval by parties other than the University and authorised agents?

    c. Will the provider notify the University of security incidents?

3. 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?

4. Data Ownership
    a. Does the University retain legal ownership of the data or information?

    b. Does the University have the right to access, control, and delete data or

information held in the cloud?

c. Does the University have any control over subcontracting by the Cloud Computing provider?

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. University's risk appetite
    a. Will the consequence be within the University's risk appetite?

4 References

Nil.

5 Schedule Information

Accountable Officer	Executive Director (ICT Services)
Responsible Officer	Executive Director (ICT Services)
Policy Type	University Procedure
Policy Suite	ICT Information Management and Security Policy
Approved Date	20/10/2017
Effective Date	20/10/2017
Review Date	1/5/2018
Relevant Legislation	*Copyright Act 1968* (Cwlth) *Crime and Corruption Act 2001* *Defence Trade Controls Act 2012* (Cwlth) *Information Privacy Act 2009* Information Standard 18: Information Security

	Information Standard 26: Internet Information Standard 40: Record Keeping Information Standard 44: Information Asset Custodianship Metadata Management Principles *Public Records Act 2002* (Qld) *Right to Information Act 2009* (Qld)
Related Policies	Administrative Access Scheme Policy Business Continuity Policy Contract Management Policy (under development) Enterprise Architecture Policy Intellectual Property Policy and Procedure Privacy Policy Procurement Policy Records and Information Management Policy Right to Information Policy Risk Management Policy and Procedure
Related Procedures	Administrative Access Scheme Procedure Information Asset and Security Classification Procedure Records and Information Management Procedure Right to Information Procedure
Related forms, publications and websites	A Guide to Implementing Cloud Services - Better Practice Guide Cloud Computing Security Considerations Negotiating the cloud - legal issues in cloud computing agreements Privacy Impact Assessment Privacy Threshold Assessment

Definitions	**Terms defined in the Definitions Dictionary**
	University The term 'University' or 'USQ' means the University of Southern Queensland.
	Definitions that relate to this schedule only
	Cloud Computing A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Keywords	
Record No	15/362PL