Cloud Computing Engagement Schedule

University of Southern Queensland

1 Purpose

To provide the Information System Custodian or their nominee with a checklist to be used in conjunction with information provided in the Engagement of Cloud Computing Services Procedure.

2 Scope

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

3 Schedule

By acknowledging completion of the items in this checklist, the Information System Custodian confirms that consideration of the key actions has been undertaken.

Relevant Section within Procedure		**Check/Tick**
	Build a business model to provide business context, estimate lifecycle cost and to form the basis for functional, performance and resource requirements	
	Capture requirements for functionality, standards, performance, manageability, security and compliance	
	Build a business case, providing business rationale and an assessment of options	
4.1	**Assess the risks** and determine suitable treatment strategies	
4.1.1	**Evaluation and Consultation** with relevant stakeholders	
4.1.2	Consider issues relating to **Intellectual Property and Copyright**	
4.1.3	Consider **Location of provider and relevant infrastructure** for data sovereignty	
4.1.4	Consider **Privacy and Data Security**	

Failure to comply with this Policy or Policy Instrument may be considered as misconduct and the provisions of the relevant Policy or Procedure applied. A hard copy of this electronic document is uncontrolled and may not be current as UniSQ the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the UniSQ's Policy and Procedure Library.

4.1.5	Consider **Records Retention and Availability**	
4.1.6	Consider **Data Classification**	
4.1.7	Consider **Business Continuity**	
4.1.8	**Determine contractual terms** prior to engaging the market	
4.1.8	**SLA and prepare an exit strategy** which considers business continuity, disposition of data and exit costs	
	Approach the market	
	Select a provider, verifying claims on costs, architecture, reputation and capability	
	Plan the implementation, ensuring sufficient resources to prepare infrastructure and manage organisational change	
	Prepare for on-going operations, ensuring sufficient in-house resources will be in place for on-going operations	
	Manage and Review the contract, service and vendor relationship on an on-going basis at pre-defined time intervals.	

4 References

Nil.

5 Schedule Information

Accountable Officer	Chief Digital Information Officer
Responsible Officer	Chief Digital Information Officer
Policy Type	University Procedure
Policy Suite	Business Continuity Policy
Approved Date	20/10/2017
Effective Date	20/10/2017
Review Date	17/10/2028
Relevant Legislation	
Policy Exceptions	Policy Exceptions Register
Related Policies	Administrative Access Scheme Policy

Failure to comply with this Policy or Policy Instrument may be considered as misconduct and the provisions of the relevant Policy or Procedure applied. A hard copy of this electronic document is uncontrolled and may not be current as UniSQ the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the UniSQ's Policy and Procedure Library.

	Contract Management Policy (under development) Enterprise Architecture Policy Enterprise Risk Management Policy ICT Information Management and Security Policy Intellectual Property Policy Privacy Policy Procurement Policy Records and Information Management Policy Right to Information Policy
Related Procedures	Administrative Access Scheme Procedure Commercialisation of Intellectual Property Procedure Engagement of Cloud Computing Services Procedure Information Asset and Security Classification Procedure Intellectual Property Procedure Privacy 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**
	Information System Custodian An individual or group of people who have been officially designated

	as accountable for specific data that is transmitted, used, and stored on a System within the University.
	Definitions that relate to this schedule only
Keywords	
Record No	15/363PL

Failure to comply with this Policy or Policy Instrument may be considered as misconduct and the provisions of the relevant Policy or Procedure applied. A hard copy of this electronic document is uncontrolled and may not be current as UniSQ the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the UniSQ's Policy and Procedure Library.