Engagement of Cloud Computing Services Procedure

1 Purpose

To establish the processes that University Information System Custodians must follow when considering the engagement of Cloud Computing services and service providers.

2 Scope

This procedure applies to all University Information or Information Systems which are stored with or hosted by any party other than the University within one of its Data Centres.

3 Procedure Overview

This procedure provides the process to be followed when considering and before making a decision to contract Cloud Computing services such as:

- Applications As A Service (AaaS)/Software As-A-Service (SaaS)
- Platform-As-A-Service (PaaS)
- Infrastructure-As-A-Service (IaaS).

4 Procedures

Consistent with the principles provided in the Enterprise Architecture Policy, it is the University's preferred position to adopt and use Cloud Computing services first, with all new services deployed in the cloud where possible.

4.1 Risk assessment

The Information System Custodian must conduct a risk assessment when considering the use of Cloud Computing services. The extent of the 'risk assessment' must be commensurate with the Information Security Classification of the Cloud Computing service under consideration (refer to the Information Asset and Security Classification Procedure).

As a first step, the Information System Custodian must consider whether the selection of a Cloud Computing service is appropriate given the Information Security Classification (refer to the Information Asset and Security Classification Procedure) associated with the Information System under consideration. With reference to the Cloud Service Use Inherent Risk Schedule

determine whether the University should be considering a Cloud Computing service and the level of rigor that should be applied in this and subsequent processes before selecting a Cloud Computing provider.

External agencies such as the Australian Department of Defence Intelligence and Security and the Australian Government Information Management Office provide a range of questions to identify the risks associated with Cloud Computing and determine suitable treatment strategies. The Information System Custodian should also consider the cost to manage the associated risks and its impact on the value proposition.

The following risk categories should be used when identifying risks:

- quality - does the cloud solution meet stakeholder needs
- financial - does the cloud solution provide value for money
- organisational - does the cloud solution work within the University's culture
- integration - can the cloud solution meet objectives without business or technical integration difficulties
- compliance - does the cloud solution comply with University's legal, regulatory and policy obligations
- business continuity - can the cloud solution recover from outages or disaster situation
- external - is the Cloud Service Provider's performance adequate.

The Cloud Computing service provider and all subcontractors in the service provision supply chain must be subject to the risk assessment and conditions on the service agreement/contract.

Each of the factors below should be addressed when preparing a risk assessment for proposed Cloud Computing deployments. Refer to the Cloud Computing Engagement Schedule for a checklist to assist in preparation of the risk assessment.

4.1.1 Evaluation process

Information System Custodians should use the Cloud Computing Engagement Schedule as the basis for evaluating the implementation of a potential Cloud Computing solution. When deciding to use a Cloud Computing service or to store Information or data in a facility which is not owned by the University, it is the responsibility of the Information System Custodian to consult with other appropriate Information System Custodians, process owners, stakeholders, and subject matter experts during the evaluation process.

The Legal Office, Procurement Office, University Privacy Officer, Manager (Enterprise Information Management Services) and the Executive Director (ICT Services) must be

consulted for guidance.

4.1.2 Intellectual property and copyright

Information System Custodians should refer to the Intellectual Property Policy and Procedure to ensure that Information or data is not stored in any facility where the University's intellectual property, copyright, trademarks or patents may be compromised.

Information or data must not be stored in such a way that allows unauthorised parties to claim ownership of the Information or data.

4.1.3 Location of provider and relevant infrastructure

Due to the nature of web-based services, providers or their equipment will often be based interstate or overseas. If any data is to be hosted or stored outside the University, the Information System Custodian must check where this will be, who will have access, who will be managing this and how. Depending on the response, additional terms and conditions may need to be included in the legal contracts to mitigate any potential risks. Providers should notify the University if any of these conditions change during the agreement. Data stored outside Australia may be subject to different laws, which could affect University compliance requirements, such as privacy.

Use of three-way encryption (upload, download and storage) should be considered to improve data security.

4.1.4 Privacy and Data Security

The University is subject to the *Information Privacy Act 2009* which specifies conditions regarding the use and handling of Personal Information as defined in that Act. If any Personal I nformation is to be collected by, or disclosed or transferred to the service provider, the Information System Custodian needs to make sure it meets these requirements. The Information System Custodian can assess these requirements by undertaking a Privacy Threshold Assessment (PTA) and, if required, a Privacy Impact Assessment (PIA).

Performing a PTA enables the Information System Custodian to quickly assess whether Personal Information is involved. Advice on completing a PTA can be sought from the University Privacy Officer or Manager (Enterprise Information Management Services). Once completed, it is recommended that a copy of the PTA be forwarded to the University Privacy Officer for endorsement and recording.

If Personal Information is involved, a PIA should be completed (effort commensurate with the risk) at the discretion of the Information System Custodian and/or University Privacy Officer following the outcome of the PTA. Resources to assist with the conduct of a PIA and guidance on Cloud Computing and privacy compliance are available - refer to Section 7 Procedure Information for details.

To fulfil its privacy obligations the University must take reasonable steps to protect Personal

Information from misuse, loss, unauthorised access, modification or disclosure. For local suppliers, the University will usually need to impose contractual requirements to ensure relevant laws apply.

Extra protection may be needed if providers or equipment are based outside Australia or overseas. Local protections may not be as strong or may conflict with University requirements. For example, under US law the US Government may be able to require access to data without notifying the relevant owner. Personal Information should not be transferred outside of Australia without taking reasonable steps to gain the 'informed consent' of the persons.

For transfers outside Australia, the University may need to consider whether it reasonably believes the other party will be subject to substantially similar to Queensland privacy principles. If that is not the case, extra steps are to be taken to ensure adequate protections are in place.

If a Cloud Computing provider deals with any University Information (for example storing, transferring or accessing it) the Information System Custodian should check that there will be adequate controls in place for security and access to that data. In the case of Research data and information, this may be covered by the Australian Research Council (ARC) and may fall under the respective Research Integrity and Ethics guidelines of the Australian Health Ethics Committee (AHEC), Human Research Ethics Committee (HREC) or National Health and Medical Research Council (NHMRC).

The University will retain ownership of University Information irrespective of where it is stored. Information and Communication Technology (ICT) Services should be consulted where any security issues are unclear.

Relevant data security issues for the Information System Custodian to consider include:

- data control
- data encryption
- blending of data with other customer data
- business process if a security breach does occur or if data is damaged or destroyed
- data backup frequency/conventions/standards/accessibility
- availability of an audit trail to demonstrate that University data is reliable.

Relevant data access issues for the Information System Custodian to consider include:

- quick and easy access
- format useability

- process to follow if data cannot be accessed or access is delayed
- ease with which the data can be amended or deleted if required.

Information or data that has been marked as Restricted Information must be stored in a way that minimises the likelihood that the Information or data can be accessed by any unauthorised parties.

4.1.5 Records retention and availability

All University records including but not limited to teaching, research and administrative records must be stored, retained and accessed in accordance with relevant legislation and University's Records and Information Management Policy.

4.1.6 Data classification

Data classification should determine the appropriate type of Cloud Computing service that may be used by the University.

Data to be considered for a Cloud Computing service must be classified according to the Information Asset and Security Classification Procedure.

4.1.7 Business continuity

1. The Information System Custodian must ensure the continuity of service for every system with a Cloud Computing provider. This requires the Information System Custodian to:
    a. determine if the Cloud Computing provider's business continuity and disaster recovery plan is acceptable

    b. determine the impact of outages

    c. ensure the availability of data in the event of any and all types of outage (e.g. through off site backup data that is accessible to the organisation)

    d. prepare a business continuity plan for both short and long term

    e. include scheduled outages in service level agreements

    f. arrange a guarantee of availability

    g. consider the use of multiple Cloud Computing providers depending on the business criticality of the system deployed to the cloud

    h. determine whether Information is able to be retrieved or disposed of in

compliance with the *Public Records Act 2002* during or at the conclusion of a contract with the Cloud Computing provider.

4.1.8 Legal issues

Prior to approaching the market, the Information System Custodian should determine the contractual terms required, even when it is anticipated that a standardised 'click wrap' agreement will be the only option. A prior understanding of the University's terms will provide a basis to ensure the final contract will meet business requirements, security requirements and adequately address the risks associated with the cloud solution.

The Information System Custodian should consult with the Executive Director (ICT Services), Manager (Enterprise Information Management Services), Legal Office or the University Privacy Officer to establish a Service Level Agreement (SLA) with the vendor. At a minimum the SLA will include:

1. clear definition of services
2. agreed upon service levels including service availability time, service outages, routine maintenance timeframes, upgrades and changes to the cloud computing services
3. clearly defined physical and logical security conditions
4. performance measurement
5. problem management
6. customer duties
7. disaster recovery
8. termination of agreement
9. protection of sensitive Information and intellectual property
10. agreement of the disposal of Information when required
11. definition of vendor versus customer responsibilities, especially pertaining to backups, incident response, and data recovery.

The Information System Custodian should refer to 'Negotiating the cloud - legal issues in cloud computing agreements' as a starting point for defining contractual terms. This guide details the contractual mechanisms to manage risks (refer to Section 7 Procedure Information).

An exit strategy for disengaging from the vendor and/or service should be planned before committing Information or data to a Cloud Computing or outsourced service. The exit strategy should outline how the relevant records will be preserved and maintained, and how the service can be discontinued or transitioned to another provider.

Risk management of these issues needs particular attention if any data or system is outside the legal jurisdiction of Queensland and/or Australia. Contracts and/or agreements are to cover the Cloud Computing provider and all subcontractors involved in providing the Cloud Computing service.

The University should consider including the need for vulnerability assessment/penetration testing in any contracts/agreements with Cloud Computing service providers. This is mandatory when Restricted Information is involved.

5 References

Australian Government Department of Finance and Deregulation Australian Government Information Management Office. (2013). *Negotiating the Cloud - Legal Issues in Cloud Computing Agreements - Better Practice Guide.* Retrieved February 17, 2015, from http://www.finance.gov.au/sites/default/files/negotiating-cloud-legal-issues.pdf.

6 Schedules

This procedure must be read in conjunction with its subordinate schedules as provided in the table below.

7 Procedure 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
Subordinate Schedules	Cloud Computing Engagement Schedule Cloud Computing Use Inherent Risk Schedule
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,	A Guide to Implementing Cloud Services-Better Practice Guide

publications and websites	Cloud Computing Security Considerations Privacy Impact Assessment Privacy Threshold Assessment
Definitions	**Terms defined in the Definitions Dictionary**
	Information Any collection of data that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form. Information Classification Classified data represents data classified as either Public Information, Internal Information or Restricted Information in this document. The classification of an Information Asset is to identify Security Controls required to protect that asset. Information Security Concerned with the protection of Information from unauthorised use or accidental modification, loss or release. 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. Information Systems The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information. Internal Information Information should be classified as Internal when the unauthorised disclosure, alteration, or destruction of that Information could result in a moderate level of risk to the University. By default, all Information Assets that are not explicitly classified as Restricted Information or Public Information should be treated as Internal Information. A reasonable level of Security Controls should be applied to Internal

Information. Access to Internal Information must be requested from, and authorised by, the Information System Custodian. Access to Internal Information may be authorised to groups of persons by their job classification or responsibilities (e.g. role-based access). Internal Information is moderately sensitive in nature. Often Internal Information is used in making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the University should this information not be available when needed is moderate.

Personal Information

Is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Public Information

Information should be classified as Public when the unauthorised disclosure, alteration, or destruction of that Information would result in little or no risk to the University. While little or no controls are required to protect the confidentiality of Public Information, some level of control is required to prevent unauthorised modification or destruction of that Information. Public Information is not considered sensitive; therefore, it may be granted to any requestor or published with no restrictions. The integrity of Public Information should be protected and in particular, the growing social media phenomenon casts doubts on the messages contained within. The appropriate Information System Custodian must authorise replication or copying of the Information in order to ensure it remains accurate over time. The impact on the University should Public Information not be available is low.

Restricted Information

Information should be classified as Restricted when the unauthorised disclosure, alteration, or destruction of that Information could cause a significant level of risk to the University or its affiliates. Restricted Information includes Information protected by the State or Commonwealth privacy regulations and Information protected by confidentiality agreements. The highest level of Security Controls should be applied. Access to Restricted Information must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job (e.g. need-to-know). Access to Restricted Information must be individually requested and then authorised in

	writing by the Information System Custodian. Restricted Information is highly sensitive and may have personal privacy considerations, or may be restricted by law. In addition, the negative impact on the institution should this Information be incorrect, improperly disclosed, or not available when needed, is very high. University The term 'University' or 'USQ' means the University of Southern Queensland.
	Definitions that relate to this procedure only
	Applications-As-A-Service (AaaS)/Software-As-A-Service (SaaS) Provides access to software. Users can log-on from anywhere and have full access to their specific software in the cloud. A common use of SaaS is cloud-based e-mail. **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. **Infrastructure-As-A-Service (IaaS)** Provides computing hardware such as servers, network equipment, and data storage on a scalable basis in the cloud. A common use of IaaS is cloud-based backup and recovery. **Platform-As-A-Service (PaaS)** Provides an application development environment that allows users to collaborate, develop, test, deploy, host and maintain applications in the cloud. A common use of PaaS is cloud-based environments for the development of enterprise-level software.
Keywords	
Record No	14/2646PL