Adopting Cloud-based Services - Procedures

1. Purpose of procedures

This document is intended as a high-level Cloud-based Services statement for use by all University staff and users of the University's information and communications resources.

These procedures apply to any University acquisition of Cloud-based Services and pertains to the acquisition of IT services from a source or sources outside of the University. While these procedures are predominantly relevant when acquiring services, they are also applicable for freely available services in circumstances where that service is critical to the operations of the University.

The purpose of these procedures is neither to promote nor discourage the engagement of Cloud-based Services but to provide guidance for the evaluation and when appropriate the engagement of Cloud-based Services.

2. Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to these procedures and are critical to its effectiveness:

Cloud-based Services is a generic term used to define a range of Internet-accessible computing resources. This spans a wide variety of service options and for the purposes of this procedure includes, but is not limited to:

Internally hosted and Private Cloud based services are data and information storage hosting services that are delivered on-campus or via University managed facilities.

Externally hosted, Public Cloud and Cloud Hosted are the most commonly known and understood forms of Cloud-based Services, where some or all components of the service are provided and managed by third parties.

Business Process as a Service (BPaaS) is Business Process Outsourcing (BPO) that employs a Cloud-based Service model.

Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is hosted as a Cloud-based Service by a third party.

Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualised computing resources as a Cloud-based Service.

Platform as a Service (PaaS) is a category of Cloud-based Services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining on-premise infrastructure traditionally associated with developing and delivering an application.

3. Procedures

The University will adopt and use Cloud-based Services subject to evaluation similar to any other ICT service but only after the additional issues associated with this delivery model, such as information privacy and security have been considered and the risk profile identified and mitigation strategies developed.

3.1 Total cost of ownership

The total cost of ownership, with an emphasis on shifting costs from capital to recurring expenditure, must be taken into consideration in the procurement or adoption of all information technology and associated services. While the use of Cloud-based Services may reduce the initial cost impediment to implementing new systems the total cost of ownership must be of prime consideration when comparing Cloud-based Services with internally hosted services.

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Information Officer

FIRST APPROVED

8 August 2017

LAST AMENDED

26 August 2024

REVIEW DATE

8 August 2022

STATUS

Active

3.2 Adherence to legislation

The University's use of Cloud-based Services must adhere to relevant legislation associated with State and Federal information management including issues of privacy, records management, and any other applicable requirements, such as, copyright, financial, ownership and geo-location of data.

3.3 Contractual controls

The holding of University data and information on externally hosted Cloud-based Services requires appropriate contractual agreements be in place and University authorisation for the data to be stored off site. This is of particular importance where University data and information is stored off-shore by organisations not bound by Australian Privacy Legislation.

In particular, specific consideration of University policy and procedures in relation to information management and research data is required by individuals when confidential and restricted University data and information is to be stored in external repositories that do not have contractual agreements in place with the University (e.g. Dropbox). See the Cloud-based Services process available on MyUniSC (staff login required).

3.4 Information and records management

Data and information stored on externally hosted cloud services remain information assets of the University. These assets need to be managed appropriately, in accord with the Information Management Framework – Governing Policy and associated procedures.

3.5 Risk assessment

The use a Cloud-based Services leaves the University more vulnerable to the fate of the Cloud-based Service provider. This additional risk factor needs to be considered when choosing a Cloud-based Service and appropriate risk analysis and mitigation strategies considered.

Cloud-based Services present additional levels of risk to the confidentiality, integrity, and availability of data. It is expected that the level of physical, technical, and administrative safeguards provided by the supplier are commensurate with the sensitivity and criticality of those information assets and services. Safeguards are essential to help protect the reputation of the University and reduce its exposure to legal and compliance risks throughout the lifecycle of the data.

A checklist is available to outline the considerations necessary for assessing Cloud-based Services, together with the safeguards that may be required, and can assist with preparing requests for information from Cloud-based Service providers.

3.6 Approvals

The procurement or adoption of Cloud-based Services, including the negotiation of contractual agreements and the assessment of risk must be co-ordinated through Information Technology.

As with all ICT procurement the Government Information Technology Contracting (GITC) framework is preferred for all ICT contractual agreements.

Any exemptions to the application of these procedures needs to be authorised in writing by the Director, Information Technology.

END

RELATED DOCUMENTS

- Critical Incident Management - Operational Policy

- ICT Access Control - Operational Policy
- ICT Security - Operational Policy
- Incident Management - Procedures
- Social Media - Operational Policy
- Social Media - Procedures

LINKED DOCUMENTS

- ICT Access Control - Operational Policy

RELATED LEGISLATION / STANDARDS

- Queensland Information Standards
- Information Privacy Act 2009 (Qld)
- AS ISO 15489 Records Management
- AS ISO/IEC 27001 IT Security