Cloud Hosting Policy

Approving authority	Vice Chancellor
Approval date	18 May 2019
Advisor	Naveen Sharma | Senior Manager, IT Risk and Compliance n.sharma@griffith.edu.au | (07) 373 57601
Next scheduled review	2021
Document URL	http://policies.griffith.edu.au/pdf/Cloud-Hosting-Policy.pdf
TRIM document	2019/0000089
Description	This policy sets out the principles, objectives and responsibilities for externally hosting services or data by anyone within the University.

Related documents

Authority to Sign Contracts and Agreements: Schedule of Delegations
Enterprise Information Systems Policy
Information Security Policy
Queensland State Archives Brief - Managing the Recordkeeping Risks Associated with Cloud Computing
Records Management Policy
Risk Management Policy
Information Technology Code of Practice
Griffith University Privacy Plan
Take Down Notice Procedure
Social Media Guidelines

1. DEFINITIONS

a) Internally hosted and Griffith private cloud are data and information storage hosting services that are delivered on-campus or via Griffith University managed facilities.

b) External hosting, commonly known as cloud computing, is where some or all components of the service are provided and managed by third parties.

2. PREAMBLE

Cloud computing has become a mainstream computing service delivery alternative. According to the National Institute of Science and Technology (NIST)[1], cloud computing has five characteristics[2], and can be defined as: “a model for enabling 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.” Three common service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Use of cloud computing at Griffith University encompasses both production services and project lifecycle environments (e.g. development, testing, quality assurance, acceptance and production)

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[2] On-demand self-service; ubiquitous network access; location transparent; resource pooling; rapid elasticity; and measured service with pay per use

and may offer benefits in the cost, performance, and delivery of IT services. The use of cloud computing services has grown and will continue to grow significantly.

3. POLICY STATEMENT

The primary reason for this policy is to facilitate a managed and co-ordinated adoption of cloud computing services by providing appropriate governance and oversight.

As the preferred option, Griffith will adopt and use cloud computing services subject to business case and privacy considerations and only after issues of security and risk management have been identified and mitigated against.

The total cost of ownership, with an emphasis on shifting costs from capital to approved recurring expenditure, must be taken into consideration in the procurement or adoption of all information technology and associated services.

Griffith's use of cloud computing services must adhere to relevant legislation associated with State and Federal information management including issues of privacy, legal, records management, and any other applicable requirements, such as, copyright, financial, ownership and geo-location of data.

The holding of University data and information on externally hosted cloud computing services requires appropriate contractual agreements be in place and University authorisation for the data to be stored off site.

University data and information must not be stored in external repositories that do not have formalised or contractual agreements in place with the University. Any exceptions to this would require approval by the Vice President (Corporate Services) on the recommendation of the Chief Digital Officer.

Data and information stored on externally hosted cloud services remain corporate assets of Griffith University. These assets need to be managed appropriately, in accord with Griffith's Records Management Policy.

The procurement or adoption of cloud computing services, including the negotiation of contractual agreements and vendor management must be co-ordinated through the Chief Digital Officer, Digital Solutions. The approval of the Vice President (Corporate Services) is required for adoption of a cloud based service whether it is for the replacement for an existing system or service or for procurement for a new system or service.

Any exemptions to the application of this policy need to be authorised in writing by the Chief Digital Officer (or delegate).

4. SCOPE

This policy applies to any Griffith University acquisition of cloud computing services and pertains to the acquisition of services from a source outside of the University, regardless of whether it is free or based on a subscription model. Internally hosted cloud computing services are already covered by existing process and policies.

An established exception to this policy is use by the Griffith community of University authorised social media platforms that allow user content to be uploaded or modified (e.g. YouTube) without compromising Griffith's copyright guidelines, Social Media Guidelines, IT Code of Practice and using University information computing resources.

5. POLICY OBJECTIVES

The objectives of this Cloud Hosting Policy are to ensure:

a) Compliance with relevant legislation and policies, i.e. that the use of externally hosted services is managed in accordance with applicable State and Federal regulatory requirements and Griffith University Policies and guidelines.

b) An appropriate level of oversight is provided, to address the possibility of a higher level of risk existing as a result of these new service models.

c) Risks are identified, prioritised and managed in a coordinated manner.

d) Where the confidentiality, integrity, and availability of data are at risk, 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 and match the levels of those provided in-house. Such safeguards are essential to mitigate against data breach to prevent serious harm to individuals and help protect the reputation of the University and reduce its exposure to legal and compliance risks throughout the lifecycle of the data;

e) Effort is not duplicated (existing internal and external options should be explored prior to acquiring a new service), nor ownership of the University's assets compromised;

f) Co-ordination and appropriate interfaces exist, and that system design is in line with Griffith architectural principles and standards.

g) The University's information assets remain protected and available.

h) The University derives maximum value from expenditure on IT services.

6. RESPONSIBILITIES

For execution of cloud service contracts the Griffith University Authority to Sign Contracts and Agreements: Schedule of Delegations is applicable.

The approval of the Vice President (Corporate Services) is required prior to execution of any cloud service contracts. In granting this approval, the Vice President (Corporate Services) shall seek advice and recommendations from the Chief Digital Officer. Exceptions to this requirement include: when there is no impact on the electronic infrastructure recurrent budget; the hosted service does not contain restricted data based on Griffith University data classification principles (that is, Sensitive and Protected). In these situations, the CDO or (delegate) are able to approve cloud service contracts.

Risk analysis of compliance, financial and contractual risks are undertaken by Digital Solutions, Finance, and Legal Services prior to contract execution.

On an ongoing basis, operational and contractual risks are to be managed by the relevant Business Owner and Data Custodian for that cloud service.

Managers, at all levels, are required to ensure that staff and students are aware of their responsibilities under the Information Technology Code of Practice.

7. MONITORING, REPORTING AND REVIEW

While providing benefits to the University, implementation of cloud services can also introduce risks. As risks are identified, they must be managed through the use of the Digital Solutions IT Risk Register. The Senior Manager, Risk and Compliance is responsible for maintaining the Digital Solutions IT Risk Register and reporting monthly to the Chief Digital Officer.

Any significant IT risks associated with hosted services must be escalated immediately to the Chief Digital Officer.

The Chief Digital Officer will report regularly on the utilisation of cloud computing services and on any significant IT risks associated with hosted services, to the Vice President (Corporate Services).

As part of its scheduled audits, the Internal Audit section is responsible for reporting to the Audit Committee on IT risk management, as it relates to controls and processes for hosted services.

This policy will remain in effect until reviewed, which will be undertaken by the University's Senior Manager, IT Risk and Compliance every two years or sooner as deemed appropriate based on implementation and use of digital assets or changes in regulatory requirements.