Information Security Policy

Approving authority	Vice Chancellor
Approval date	19 March 2014
Advisor	Naveen Sharma | Manager, IT Architecture and Compliance | Division of Information Services (INS) N.Sharma@griffith.edu.au | (07) 373 57601
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Information Security Policy.pdf
TRIM document	2014/0003526
Description	This policy sets out the principles, objectives and responsibilities for information security management within the University.

Related documents

Code of Conduct
Compliance Framework
Enterprise Information Systems Policy
Griffith University Code for the Responsible Conduct of Research
Griffith University Privacy Plan
Griffith University Information Technology Code of Practice
Guidelines on Appropriate Use of Administrator Access to Information Resources
Information Security Policy - Schedule A: Roles, Standards and Operational Procedures
Risk Management Framework
Risk Management Policy
Student Academic Misconduct Policy
Information Standard 18: Information Security (IS18)
ISO 27001 Information Security Management Standard, 2005

[Definitions] [Purpose] [Scope] [Policy Statement] [Policy Objectives] [Responsibilities] [Enforcement] [Monitoring, Reporting and Review]

1. DEFINITIONS

Available from the Glossary on the Information Management Framework website: http://www.griffith.edu.au/information-management-framework/glossary

2. PURPOSE

This document is intended as a high-level information security policy statement for use by all University staff, students and users of the University's information resources. All information technology resources are the property of Griffith University, unless otherwise stated in a contractual agreement. Griffith's information resources and systems are valuable University assets and must be protected and managed to ensure their security in terms of confidentiality, integrity and availability.

The purpose of this policy is to ensure:

- The provision of reliable and uninterrupted Information Technology (IT) services;
- The integrity and validity of data and information;

- An ability to recover effectively and efficiently from disruption;
- The protection of all the University's IT assets including data, information, software and hardware; and
- A consistent approach to information security management is adopted within the University.

The policy was developed with reference to Queensland Government Information Security Guideline (IS18) and the Information Security Management Standard (ISO 27001).

3. SCOPE

This Policy applies to all University staff, students and users of the University's information resources including contractors, third-party Agents of the University, as well as any other University affiliate who is authorised to access institutional data or information. It includes resources hosted on-campus or externally.

4. POLICY STATEMENT

The University recognises that information security management is an integral part of good management practice and is committed to establishing an organisational culture that ensures information security management is embedded in University activities and business processes.

The University manages information security within a broad security assurance framework. Information security risks are managed taking into account of broader University objectives and priorities.

Operationally, information security risks are managed using an IT Risk Register, in accordance with this Policy and with information risk management processes established by the University.

The University has guidelines, procedures and controls to address information security management across all operations. These help coordinate information security efforts, both electronic and physical, in a coherent, consistent and cost-effective manner. This policy should be read in conjunction with Information Security Policy Schedule A – Roles, Standards and Operational Procedures, the Enterprise Information Systems Policy and the Griffith University Information Technology Code of Practice.

Any exemptions to the application of Griffith’s established security practices need to be authorised in writing by the Chief Technology Officer (or delegate).

5. POLICY OBJECTIVES

The objectives of this policy are to ensure:

a) University executive and senior management can make informed business decisions based on appropriate security risk assessments when it involves information or data from a confidentiality or integrity perspective;

b) Information security risks are identified, prioritised and managed in a coordinated manner;

c) Strategic planning processes are improved as a result of a structured consideration of information security risk;

d) Compliance with relevant legislation; and

e) University data and information resources are safeguarded.

6. RESPONSIBILITES

The Pro Vice Chancellor (Information Services) is responsible for the implementation of information risk management within the University, and will report regularly to the Vice Chancellor on any significant information security risks or on strategic information risk areas.

The Chief Technology Officer oversees information security risk management and security assurance activities within the University, as delegated b the Pro Vice Chancellor (Information Services).

All managers and staff are responsible for management of information security risks relevant to their areas of responsibility. Managers at all levels are required to create an environment where managing information security risk is accepted as the personal responsibility of each member of the University.

7. ENFORCEMENT

Violations of this Policy or related policies, scheduled, standards or guidelines may result in suspension or loss of privileges, with respect to University data, information and information systems, after consideration by the relevant delegated University authority. Additional administrative sanctions or legal actions may apply.

8. MONITORING, REPORTING AND REVIEW

The Pro Vice Chancellor (Information Services) will report any strategic or significant information security risks, as and when required, to the Vice Chancellor.

The Pro Vice Chancellor (Information Services) will provide a status update on IT audit actions and recommendations regarding information security risk to the Audit Committee, as and when required.

The Policy will remain in effect until reviewed which will be undertaken by the Manager, IT Architecture and Compliance at least every five years or sooner as deemed appropriate based on changes in technology or regulatory requirements.