Griffith UNIVERSITY
Queensland, Australia

Policy

Information Security

1.0 Purpose

This policy describes the University's approach to information security and protection of University information technology resources.

2.0 Scope

This policy covers all University information technology resources and applies to the following user groups:

- Griffith University employees, students and alumni
- contractors and third parties providing services to the University
- any affiliates authorised to access University data or information.

3.0 Policy statement

The University is committed to ensuring information security in accordance with the following principles:

a. Griffith information technology resources are strategic assets that the University relies on for the purposes of teaching, learning, research and all administrative and business-related functions and operations.

b. Griffith information technology resources must be appropriately managed and protected to ensure confidentiality, integrity and availability.

c. Risks to information security must be managed against a range of threats through a documented and approved information security program to protect business continuity and the University's reputation. (See Section 3.1)

d. All users of Griffith information technology resources have a role to play in information security in accordance with this policy and must be aware of and execute their responsibilities.

e. This policy is supported by a range of related policies and procedures and should be read in conjunction with the Information Security Procedure and the IT Code of Practice Policy.

3.1 Information Security Program

Information Security at Griffith University is managed as an established and approved information security program, using the NIST Cyber Security framework to align with the QLD government (IS18:2018) and the internationally recognised ISO/IEC 27001 standard for an Information Security Management System (ISMS).

The 27001 standard for an Information Security Management System refers to fourteen domain areas for governance of information security. These domain areas provide accompanying control guidelines for continued protection and dictate how the objectives of this policy will be achieved per asset in context.

Digital Solutions will provide guidance and direction as required to ensure that the objectives of the policy are implemented in accordance with these guiding domains.

The domain areas cover the following aspects of information security:

- Information Security Policy
- Organisation of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity
- Compliance.

4.0 Roles, responsibilities and delegations

Every person associated with Griffith University has a role to play in protecting the organisation from information security risks and must comply with the responsibilities and expectations before engaging in activities that use Griffith University's information assets and resources. Specific user responsibilities for regular, day-to-day activities are specified in the Information Security Procedure.

All Griffith University staff are responsible for identifying and managing information security risks relevant to the information that they own, manage, store or distribute. Griffith University management - at all levels - must facilitate an environment where managing information security risk is accepted as the personal responsibility of each member of the University.

The Information Security Program provides more detailed governance and operational advice on control guidelines and associated responsibilities. Further guidance and direction on responsibilities associated with the Information Security Program and the relevant ISMS domains will be provided by Digital Solutions.

ROLE	RESPONSIBILITY
Chief Operating Officer	The Chief Operating Officer is accountable for information security within the University and will report regularly to the Vice Chancellor on any significant information security risks or issues.
Chief Digital Officer	The Chief Digital Officer is responsible for information security risk management and security assurance activities within the University, as delegated by the Chief Operating Officer.
Manager, Cyber Threat Defence	The Manager, Cyber Threat Defence is responsible for overseeing the day-to-day operation of the associated policy guidelines.
Senior Manager, Risk and Compliance	The Senior Manager, Risk and Compliance is responsible for maintaining the information security risk register and advising on compliance related matters.
Information System Users	All information system users are responsible for being aware of this and other related policies, fostering a culture of strong information security, ensuring they are aware of their responsibilities towards data they create, use, store and access, and being aware of common information security

	threats and how to identify, manage and report them and taking required action as appropriate.
Other	Further information on responsibilities for above as well as for Business Owners, Information System Custodians, Information System Providers, Information Asset Custodians, Information System Users, Directors, Deans, Heads of School/Department and administrators are referenced in the Information Security Procedure.

5.0 Definitions

Information Security Management System (ISMS) is a defined approach and process (a standards-based framework) which describes how information security is to be managed from a people, process and technology perspective.

Information Security means to protect and preserve the confidentiality, integrity and availability of information and protecting and preserving the authenticity and reliability of information and ensuring that users can be held accountable.

Information Security Program is the institutional establishment of an ISMS which is used for the purposes of conducting and managing an ongoing program of work related to security.

Information technology resources are the capture and collection of any Griffith University data, information systems, applications, technology resources and infrastructure, including but not limited to desktop computers, laptops, tablets, notebooks, smartphones, intranet, internet access, wired and wireless networks, voice and video systems, servers, storage devices and systems, cloud based services, all web services, all messaging and collaboration services including instant messaging, social media and email services, as well as all user credentials for accessing data and systems.

NIST is the National Institute of Standards and Technologies.

University digital information is any information and data stored in digital format that is either generated, received, stored, or distributed by the University.

Griffith UNIVERSITY
Queensland, Australia

Policy

INFORMATION

Printable version (PDF) Downloadable version (Word)

Title	Information Security Policy
Document number	2020/0000015
Purpose	This policy describes the University's approach to information security and protection of University information technology resources.
Audience	Public
Category	Governance
Subcategory	Digital Solutions
Effective date	16 June 2020
Review date	2021
Policy advisor	Manager, Cyber Security Governance, Risk and Compliance
Approving authority	Vice Chancellor

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS

Legislation	The Privacy Act Telecommunications Act 1997
Policy	Enterprise Risk Management Framework Griffith University Privacy Plan Information Security Management Standard (ISO/IEC 27001) Information Technology Code of Practice The Responsible Conduct of Research Queensland Government Information Security Guideline (IS18)
Procedures	Information Security Procedure
Local protocols	Enterprise Information Systems Guidance Information Security Classification Guidelines
Forms	N/A