GRIFFITH UNIVERSITY

Policy

Information Security

1.0 Purpose

Griffith University's information assets and systems are strategic resources that the University relies on for teaching, learning, research, and all administrative and business-related operations.

This policy describes the University's approach to information security to protect the University's information and information resources. The policy, and associated frameworks, standards, procedures and guidelines, ensures an appropriate level of security is applied to protect the confidentiality, integrity, and availability of the University's critical and sensitive information, from threats, whether internal or external, accidental or deliberate, and to satisfy legal, regulatory, contractual and stakeholder requirements related to information security and cyber resilience.

2.0 Scope

This policy and associated policies, standards, procedures, applies to:

a) The management of all matters relating to information security and cyber resilience within the University

b) All information systems and information assets owned, leased, operated or under custodial care of third parties operated on behalf of Griffith University

c) All individuals, including staff, students, alumni, contractors, or third party service providers accessing, using, holding, or managing information, information systems or IT assets, on behalf of the University

3.0 Policy Statement

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

a) Information is only used for its intended purpose.

b) Information must be protected from unauthorised access and to ensure information is only available to authorised users and systems.

c) Information must be protected from unauthorised modification or destruction and be accurate and complete.

d) Information must be protected to ensure it is available when needed.

4.0 Information Security Program

Griffith University has established a Cyber Security Governance and Management Framework to support this Information Security Policy. Griffith University's Audit and Risk Committee (ARC) and the Information Security, Risk and Compliance Committee (ISRC) support the establishment, implementation, maintenance, and continuous improvement of information security.

Information Security at Griffith University is aligned to the QLD government information security policy (IS18:2018) and internationally recognised standards and best practices including ISO/IEC 27001 standard for an Information Security Management System (ISMS) and the NIST Cybersecurity Framework.

Digital Solutions will provide guidance and direction as required to ensure the objectives of this policy within the following areas:

a) **Access control**. Access to information is appropriately authorised and restricted in accordance with the principles of least privileges and need to know.

b) **Asset management**. Information assets are identified, classified and appropriately protected.

c) **Business continuity**. Recovery and response plans are maintained and tested to minimise the impact to the University.

d) **Communications security**. Networks and information in transit is appropriately protected.

e) **Cryptography**. Confidentiality of information is appropriately protected whilst at rest and in transit.

f) **Human resource security**. Staff are appropriately screened, made aware of their information security responsibilities and provided mandatory cyber security awareness training.

g) **Information security risk management**. Information security risks are identified, assessed, and monitored.

h) **Operations security**. The daily operations of information systems and resources are appropriately protected.

i) **Physical and environmental security**. Information assets and technology are appropriately protected from physical threats and natural hazards.

j) **System acquisition, development, and maintenance**. Security is considered throughout the lifecycle of a system.

k) **Third party security**. Suppliers are appropriately screened and required to appropriately protect our information.

5.0 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.

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 promote 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 will be provided by Digital Solutions.

ROLE	RESPONSIBILTY
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 and promoting a culture of strong information security
Chief Digital Officer	Is responsible for information security risk management and security assurance activities within the University, as delegated by the Chief Operating Officer.
Director Cyber Security	Is responsible for providing advice, risk management, overseeing the day to day operations and the implementation, maintenance and improvement of relevant frameworks, policies, standards, procedures, guidelines and controls related to information and cyber security, and approving exceptions to the information security policy and associated standards and procedures.
Managers / Supervisors	Are responsible for the implementation and oversight of this policy and promoting a culture of strong information security within their area of responsibility.
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.

6.0 Policy Exceptions

a) If a product, solution, or process cannot be used or implemented in accordance with this information security policy or related frameworks, policies, standards, procedures, and guidelines, then an exception may be granted by the Director of Cyber Security to provide a temporary concession and shall be reviewed at least annually.

b) Security policy exception requests shall be considered by the Cyber Security Team and be recorded in the Cyber Security Exception Register.

7.0 Definitions

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 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 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.

NIST is the National Institute of Standards and Technologies.

8.0 Information

Title	Information Security Policy
Document number	2024/0001046
Purpose	This policy describes the University's approach to information security to protect the University's information and information resources
Audience	Public
Category	Governance
Subcategory	Digital Solutions
UN Sustainable Development Goals (SDGs)	This document aligns with Sustainable Development Goal/s: 16: Peace, Justice and Strong Institutions
Approval date	9 April 2024
Effective date	9 April 2024
Review date	2027
Policy advisor	Director of Cyber Security
Approving authority	Chief Operating Officer

9.0 Related Policy Documents and Supporting Documents

Legislation	Privacy Act
Policy	Griffith University Privacy Plan Information Technology Code of Practice Risk and Resilience Management Policy

	Queensland Government Information Security Guideline (IS18)
Standards and Procedures	Access Control and Authentication Standard *(Staff Only)* Backup Standard *(Staff Only)* Business Continuity and Disaster Recovery Standard *(Staff Only)* Cryptographic Control and Encryption Standard *(Staff Only)* Data Breach Response Plan *(Staff Only)* Information and Data Protection Standards *(Staff Only)* Information Security Classification Procedure Logging and Monitoring Security Standard *(Staff Only)* Malware Protection Standard *(Staff Only)* Network Security Standard *(Staff Only)* Physical and Environmental Security Standard *(Staff Only)* Secure System Development Standard *(Staff Only)* Third Party Supplier Security Standard *(Staff Only)* Vulnerability Management Standard *(Staff Only)*
Local Protocol	Change Management Process *(Staff Only)* Cyber Security Governance and Management Framework *(Staff Only)* Digital Technology & Cyber Security Risk Management Framework (Staff Only) Incident Management Process *(Staff Only)*
Forms	N/A