Chief Digital Officer Authority - Digital Assets

Approving authority	Vice Chancellor
Approval date	2 October 2017
Advisor	Chief Digital Officer | Digital Solutions | b.callow@griffith.edu.au | (07) 373 56433
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Chief Digital Officer Authority - Digital Assets.pdf
TRIM document	2017/0000428
Description	This policy details the actions the Chief Digital Officer (CDO) has authorisation to enact in the arena of cybersecurity and information technology operations to mitigate against unauthorised access to and loss of University information and the misuse of University digital assets.

Related documents

Data Classification Guidelines

Emergency Management Plan

Information Asset Register (Public)

Information Asset Register (Internal)

Information Security Policy

Information Technology Code of Practice

[Context] [Compliance and Exceptions] [Roles and Responsibilities] [Guideline Requirements] [Definitions]

1. CONTEXT

This policy provides authorisations for actions undertaken by the Chief Digital Officer (CDO) to safe guard the digital assets and digital information of Griffith.

This policy applies to:

- All Griffith University employees as well as contractors, temporary staff, consultants and external organisations that have been provided access to Griffith University information and information processing facilities. For the purpose of this document, the word 'user' has been used to refer to all such individuals.
- All digital information captured, provided and/or subscribed by Griffith University.
- All digital assets that are connected to the University network or utilise the University network.

2. COMPLIANCE AND EXCEPTIONS

2.1 Compliance

Business owners of information systems, custodians of digital assets, system administrators and users of Griffith University information systems are required to understand and comply with this policy. The Chief Digital Officer will monitor compliance.

2.2 Exceptions

Exceptions to this policy may be granted for reasons such as:

- Technical inability to comply with the policy;
- Existing non-compliance but under an action plan to become compliant with the policy.

Requests for exceptions to the policy must be submitted to the Chief Digital Officer for approval. A record of granted exceptions to the guidelines, their durations and their business justification will be maintained.

2.3 Non-compliance

Where deliberate breaches of guidelines are established, it will be treated as failing to comply with required duties and the matter will be dealt with under the Code of Conduct and / or the relevant policy, standard or guideline which may result in disciplinary consequences.

3. ROLES AND RESPONSIBILITIES

Role	Responsibility
Chief Digital Officer (CDO)	• The CDO as the owner of this policy is responsible for ensuring the policy is reviewed based upon a defined review mechanism. • The CDO is authorised to undertake actions in line with this policy. • The CDO is authorised to take disciplinary actions upon non-compliance with this policy. This may involve making recommendations to the relevant University Executive.
Manager of Cyber Security	• The Manager Cyber Security is responsible for actively reviewing the policy to ensure that the policy is up to date, and adding additional authorisations once approved. • The Manager Cyber Security is responsible for ensuring the activities detailed in the policy are enacted as authorised by the CDO • The Manager Cyber Security is responsible for formulating and implementing Policies, Standards, Guidelines and Procedures for protecting the University's digital assets.
System Administrators responsible for management and security of digital assets	• The staff members responsible for securing digital assets will manage and operate in a manner that reduces and mitigates vulnerabilities by adhering to relevant Policies, Standards, Guidelines and Procedures for protecting the University's digital assets.

4. GUIDELINE REQUIREMENTS

The Chief Digital Officer has responsibility for the cybersecurity operations of the University and the safe guard of the digital information and digital assets of Griffith. This policy provides measures to protect the privacy, confidentiality, integrity and availability of the University's digital assets including information systems that store, process or transmit data.

To enact this responsibility, the CDO can approve and enforce the following:

4.1 Operational

- The scanning, review or formal penetration test of digital assets and information systems.
- Permitting digital assets to be Internet accessible.
- The conduct of a broad vulnerability assessment of the University IT assets.
- The remediation of discovered vulnerabilities in IT applications, systems and digital assets.

- In consultation with the business owner, approve an exception to existing standards and controls where business benefit outweighs residual risk.
- That appropriate due diligence is conducted prior to the release or sharing of any Griffith University digital assets with another organisation.
- The suspension or termination of an individual's access to IT systems.
- Approve and enforce network security related activities including:
  - the segmentation of the University network to provide higher order security controls where criticality of the IT asset warrants the additional protection
  - the blocking of specific communications protocols from traversing the University network
  - changes to the University border access control lists to close, limit or enable specific service ports
  - changes to the University border access control lists to block or limit access by or to specific IP addresses
  - the addition or removal of web addresses to application white or black lists
- The adherence to University network standards for all IT Assets.
- That no IT Asset, regardless of ownership, is connected to the University data networks without authorisation.
- The capture and retention of relevant digital asset log data for audit, system usage and access.
- The patching of digital assets to minimise exposure to cyber security risks.
- The protection of IoT devices that provide essential or critical ancillary services.
- As needed, assign appropriate security classification to University's digital assets and recorded in the Information Asset Register.
- The protection of digital assets that create, store, process or transmit sensitive data as categorised under the University's Data Classification guidelines.
- Ensure the retirement, disposal and destruction of digital assets are undertaken in line with University's destruction/disposal and procurement guidelines.
- The backup of University digital information to minimise risk of data loss.
- Following clearance by the University privacy officer, approve access to University held information where a validated request has been received from law enforcement agencies.

4.2 Security

The CDO can approve and enforce those actions necessary to maintain a sound cyber security stance for Griffith. These include but not limited to:

- Initiate Security Incident Response procedures.
- The physical inspection of any University digital asset.
- Access to data held on University digital assets (quarantine, copy, confiscate) as part of an investigation.
- On reasonable suspicion, the revocation of access, removal of network access, and/or physical removal of a digital asset.
- The suspension or termination of Internet access for an information system or digital asset.
- Remediation activities necessary to mitigate or remove the University exposure to the security vulnerability.
- The use of third parties to assist in the investigation or remediation of a security incident.

- Where remediation activity cannot be undertaken, or cannot be undertaken in a timely manner, the suspension of network access of an information system or digital asset.
- Other actions deemed necessary to return the University digital environment to a stable and controlled status.

5. DEFINITIONS

Term	**Definition**
Business Owner	The agreed owner of an information technology application or system. Typically the owner of the supported business function or functions.
Digital Assets	Digital assets 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, smartphones, intranet, internet access, wireless network, telephone system, servers, storage arrays / systems, cloud based services, all web and network connected devices (commonly known as IoT devices), web services, instant messaging, social media and email services.
Information security	Protect and preserve the confidentiality, integrity, and availability of information. It also involves protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable.
Information system	An information system is any set of components that is used to handle information. It can include any system, service, infrastructure, or physical location that houses information.
IT Asset	For the purposes of this document, IT Asset is defined as a “Digital Asset” (refer to definition above)
Log	Record details of information or events in an organised record-keeping system, usually sequences in the order in which they occurred.
Patch	Fixes to software programming errors and vulnerabilities.
Security incident	An event that indicates the University data or IT systems may have been compromised, or existing cybersecurity controls may have failed. A security incident may lead to a security event, where there is an actual compromise or failure of control.
System administrator	A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.
University digital information	University digital information is any information and data in digital format that is either generated and/or received and/or stored and/or distributed by the University.
Vulnerability	Vulnerability refers to the inability to withstand the effects of a hostile environment.