Griffith UNIVERSITY
Queensland, Australia

Procedure

Information Security

1.0 Purpose

This document provides mandatory procedures to support the implementation of the Griffith Information Security Policy.

It defines the roles and responsibilities of all users, administrators and managers of the University's information technology resources and identifies the standards to be applied to ensure security of digital assets, information and associated resources. It also outlines required procedures for operational security management.

2.0 Scope

This procedure applies to all digital assets, digital information resources and identities in use by Griffith University. This procedure is also supported by a number of guidelines maintained by Digital Solutions based on the Information Security Management Systems (ISMS) aligned to the international standards 27001 for information security.

Information technology resources refers to, but is not limited to, information systems that have been developed at Griffith, extended from existing information systems and purchased information systems from a vendor or delivery in a “Cloud” / Software as a Service (SaaS) mode. All information technology resources are the property of Griffith University, unless otherwise stated in a contractual agreement.

This procedure includes the following user groups:

- All full time, part time, temporary or casual Griffith University employees
- All students (including those currently enrolled and alumni)
- All contractors engaged by Griffith University
- All third parties providing services to Griffith University
- Any affiliates authorised to access Griffith University institutional data or information.

3.0 Roles, Standards and Operational Procedures

Procedures in this document are mandatory and include:

- Roles and Responsibilities
- Access Control Standards
- Asset Security Standards
- Operational Security Standards
- Vulnerability and Patch Management Standards
- System Administrator Access Standards.

3.1 Roles and Responsibilities

Following is a summary of the responsibilities of those elements and/or individuals using or supporting Griffith University's information technology resources.

3.1.1 Chief Digital Officer

The Chief Digital Officer is responsible for:

- Providing specialist information security advice to the Chief Operating Officer, and other senior officials of the University
- Ensuring relevant security standards and responsibilities are developed and implemented
- Receiving reports of incidents, threats and malfunctions that may have an impact on the University's information systems
- Ensuring remedial action is taken on all reported incidents, threats, malfunctions and security breaches
- Acting as the University's representative with external bodies, including law enforcement agencies, on matters relating to IT security
- Implementing disciplinary action for inappropriate use as delegated by the relevant University policies.

3.1.2 Senior Manager Risk and Compliance

The Senior Manager, Risk and Compliance, is responsible for managing information security policy, compliance activities and the high-level IT security architecture to inform the various stakeholders. More specifically, the Senior Manager, Risk and Compliance responsibilities include:

- Developing and maintaining the University's Information Security Policy
- Overseeing the management of the IT Risk Register
- Overseeing the management of Cyber Security Risk Register
- Coordinating IT Audit activities and responses as required across Digital Solutions
- Maintaining the Data Retention Legislation (DRL) plan and providing guidance and approvals for compliance within the parameters of the plan.

3.1.3 Manager Cyber Threat Defence

The Manager, Cyber Threat Defence is responsible for managing information security standards, procedures and controls intended to minimise the risk of loss, damage or misuse of the University's information technology resources. More specifically, the Manager, Cyber Threat Defence responsibilities include:

- Establishing and implementing standards, guidelines, capabilities and related procedures for access to the University's information and systems
- Reviewing the Cyber Security Risk Register and selecting, implementing and administering controls and procedures to manage information security risks
- Distributing security report information in a timely manner to the Chief Digital Officer and other appropriate University administrators
- Liaising with external security authorities (e.g. AusCERT, State and Federal Police)
- Promoting security awareness across the broader University community.

3.1.4 Business Owners

For each centrally managed administrative system, the Business Owner is the owner of the primary business functions that the information system supports and is the system's major stakeholder. The Business Owner has the authority to make decisions related to the development, maintenance, operation of and access to the application and data and information associated with that business activity. More specifically, the Business Owner's responsibilities include:

- Ensuring that the data in the system for which they are the business owner has received an information security classification
- Ensuring that the appropriate levels of protection and security controls are applied to systems and data for which they are the business or service owner of
- Interpreting pertinent laws and University policies to classify data and information and define its level of sensitivity
- Defining required levels of security, including those for data and information transmission
- Developing guidelines for requesting access
- Reviewing and authorising access requests
- Establishing measures to ensure data integrity for access to data and information
- Reviewing usage information
- Defining criteria for archiving data and information, to satisfy retention requirements.

3.1.5 Directors, Deans or Heads of School/Department

Directors, Deans or Heads of School/Department are responsible for ensuring that the security policy is implemented within their element. These duties may be delegated; however, it is the responsibility of the DDHSDs to:

- Ensure that element employees understand security policies, procedures and responsibilities
- Approve appropriate data and information access
- Review, evaluate and respond to all security violations reported against their staff and take appropriate action
- Communicate to appropriate University elements when employee departures and changes affect computer access.

3.1.6 University's Internal Audit Office

The University's Internal Audit Office is responsible for:

- Providing an independent assessment on the adequacy of security procedures within the IT infrastructure and information systems
- Evaluating compliance with information security policy and procedures during regular operational audits of the University's information systems
- Auditing critical corporate systems on a frequent and regular basis
- Auditing System Administrator and Database Administrator privileges regularly
- Ensure adequate controls have been included in all new systems being developed or implemented at or by the University which have a software component cost exceeding $500,000 or a system where the potential revenue base would exceed $500,000.

To facilitate the above, Audit Office staff are authorised to have inquiry-only access to all information and systems owned by the University and being operated on University premises.

3.1.7 Finance Department

The University's Finance Department is responsible for:

- Assisting the University to maintain its ongoing commitment to providing the most up to date information on cardholder data and EFTPOS terminal security best practice processes
- Ensuring that all staff dealing with card information including taking payments for University products and services are aware of guidelines, roles and responsibilities for best practice processes for protecting Griffith customer's card information and University EFTPOS terminals
- Maintaining inspection and maintenance procedures associated with Point of Sale (POS) terminals
- Maintaining a list of service providers that interact with card data
- Ensuring that staff dealing with card information are trained on and carry out periodical inspection of terminals to identify potential tampering or substitution of EFTPOS related devices and to report suspected incidents.

3.1.8 Information Usage and User Responsibilities

All users of Griffith IT systems and data are responsible for:

- Ensuring personal compliance with Information Security policy and other related policies, guidelines and standards
- Taking appropriate work practice steps to ensure that safe cyber security procedures and hygiene are managed in accordance with Griffith guidelines and advice
- Ensuring that appropriate information security classification and handling is applied to Griffith data where a user is responsible for the creation, storage, access and distribution of that data
- Participating in regular annual awareness and training where provided by Griffith University to ensure capability in identifying, managing and reporting cyber security threats and risks
- Reporting security incidents to ensure that risk of incidents to Griffith are managed and minimised.

Additionally, the Information Technology Code of Practice sets out conditions for the use of the University's information technology resources. These conditions are intended to ensure that use is ethical, legal and respectful of privacy, and covers such topics as:

- What constitutes inappropriate use of the University's information technology resources
- The need to respect other users of the University's information technology resources
- Privacy limitations in a digital environment
- Copyright compliance
- Consequences of breaching the terms and conditions outlined in the Code of Practice.

The Information Technology Code of Practice should be read in conjunction with the University's Code of Conduct and Privacy Plan.

3.1.9 System, Security and Identity Management Administrators

System, Security and Identity Management Administrators must take reasonable action to assure the authorised use and security of data and information during storage, transmission and use. System Administrators are responsible for:

- Developing, maintaining and documenting operational procedures to include data integrity, authentication, recovery, and continuity of operations

- Ensuring that access to data and information and applications is secured as defined by the Business Owner
- Providing adequate operational controls to ensure data and information protection
- Ensuring that access requests are authorised
- Modifying access when employees terminate or transfer
- Communicating appropriate use and consequences of misuse to users who access the system
- Protecting sensitive files and access control files from unauthorised activity
- Performing day-to-day security administration
- Maintaining access and audit records
- Creating, distributing and following up on security violation reports.

System, Security and Identity Management Administrators must also conform to the System Administrators Guild of Australia's Code of Ethics. ***Appendix 1*** details the *Code of Ethics for System Administrators*.

3.2 Access Control Standards

Additional and more detailed guidance on Access Control standards is available from Digital Solutions in Domain Guideline D: Access Control.

3.2.1 Identification Standards

For the purposes of policy statements contained in this procedure, access IDs (i.e. staff or student numbers) will be issued in accordance with the following standards:

- Staff on confirmation of appointment and students on matriculation (offer of place) are provided with unique usernames and initial passwords
- Any other University approved and authorised users (e.g. casual, sessional, volunteer and visitor) require the relevant element Head to authorise application for access and require CDO or delegate approval. All usernames and passwords allocated within the category must include expiry dates
- A newly issued (temporary) password must be changed on first login
- Temporary passwords will have an expiry period of 48 hours. If passwords are not changed within this period, a new password will need to be requested
- Users are responsible for maintaining the security of their IDs and all activity occurring under those IDs
- Users are prohibited from sharing or disclosing their account details and the use of any shared account is prohibited unless explicitly approved in writing from the Chief Digital Officer or nominated delegate
- All account creation or system access level requests must have an accompanying authorisation, from a person with the delegated authority (usually Element Head) to authorise these types of requests
- All nonstandard account issues (visitor, guest or other affiliated account) must be approved by the either the Chief Digital Officer, the Senior Manager Risk and Compliance or the Manager, Cyber Threat Defence (or their nominated delegate)
- Accounts designed for use by more than one person (such as generic conference accounts, workstation accounts, or generic service accounts) are not normally permitted and can only be issued with the approval of the above-mentioned roles

- Approval for conference, visitor, guest or other affiliated accounts which require access to Griffith public Wi-Fi or Griffith provided Internet access must be assessed to comply with Griffith Data Retention Legislation (DRL) subscriber requirements.

3.2.2 Authorisation Standards

Accounts will be issued in accordance with the following standards:

- Only the authorised user may use an account. A user is authorised if:
  - The user is the account holder (in the case of a user account), or
  - The account is a public access account, or
  - The user's position within the University implies authorisation and the user has a demonstrated need to use the account to carry out approved activity.
- An account holder must not authorise or allow the use of their account by other persons unless the account is authorised by the Chief Digital Officer or delegate to be used as a shared account (i.e. such as an authorised conference or visitor account or an account for a shared device)
- In the event of a policy breach or other extenuating circumstances, approval to allow access to an account by persons other than the authorised account holder, must be approved by the Chief Digital Officer or delegated authority through the relevant Head of the element concerned
- In the event where an authorised user is away from work and access is required to their user data that has been deemed critical for operation of University business, reasonable attempts must be made to contact the individual to seek approval. If this is unsuccessful, authorisation must be obtained from the Head of that element and approval must be sought in writing from Chief Digital Officer or delegated authority to enable this access
- A user should only use an account for activities approved by Griffith University
- A user must not attempt to circumvent the security mechanisms of any computer system or access via unsecured network mechanisms, or by use of illegal or unauthorised devices
- As part of security assurance, the Chief Digital Officer will authorise proactive vulnerability risk assessment and scanning of the IT infrastructure to improve the University's security posture
- Where required, the Chief Digital Officer or delegated authority may take steps to monitor, suspend or investigate account or system activity where there is reasonable evidence to indicate a potential breach of policy
- The relevant Business Owner or Chief Digital Officer or delegated authority may decide to disable or remove accounts if the following events happen:
  - The account is no longer required by the account holder
  - The account holder ceases to have an association with Griffith University
  - The account is inactive for a given period of time.

3.2.3 Authentication Standards

The following standards will be applied to all systems requiring authentication:

- Passwords or approved certificates or approved public/private keys must be used for accessing all corporate systems
- Certificates should be generated from a trusted Certificate Authority (CA) where available and have a minimum key length of 2048 bit and be valid for a period of no longer than 12 months

- Public/private key pairs should be password protected and have a minimum key length 2048 bit (4096 preferred)
- Any certificates or private keys must be stored in an encrypted mode (such as encryption on hard drives or encrypted USB storage)
- User selected passwords must comply with Griffith University complexity standards and must be at least eight characters in length and alphanumeric (i.e. as a minimum must contain at least one uppercase letter and one number)
- User selected passwords must be kept unique to Griffith and not used for access to any other non-Griffith services
- Users must not select passwords for any Griffith system where they are aware the password has been publicly disclosed as a result of a data breach, regardless of the account type or source of breach
- Users are required to change passwords at first login. In situations where a login has not been attempted or the initial password has not been changed, the user account will be deemed “not-in-use” and deactivated after 6 months from date of login creation.
- At first login Users must set the answers to four secret questions, selected from a list. On subsequent password changes or when using Forgotten Password facility, Users will be required to enter date of birth and answer two secret questions
- Passwords must be changed every 180 days
- Password change application will not allow the use of the thirteen previously used passwords
- User accounts are locked for 30 minutes if more than 10 unsuccessful login attempts are recorded in a 30 minute period
- As part of password reset, the maximum number of attempts to answer their Secret Question correctly will be ten within a 30 minute period, after which the user account will be locked for 30 minutes
- Passwords must not be displayed in writing
- When logging on, users shall take precautions to ensure others do not see their password
- Passwords must not be disclosed to others
- Passwords must not be easily associated with a particular user
- Passwords must not be the same as the username
- A user who suspects that a password has been compromised must change the password immediately. The user is required to report all details of the suspected breach to IT Service Centre
- Passwords for accounts or for encrypted files must not be sent in clear text and must be sent via an approved encrypted format. LastPass is available as a secure communication channel for all staff for this purpose. Passwords must be sent via a separate communication channel to the password target
- Passwords will be aged and are automatically checked to ensure that they comply with above standards and are non-trivial. All passwords are to be stored in an encrypted format on systems and applications. Exemptions to this are to be authorised by the Chief Digital Officer or delegated authority and logged in the IT Risk Register
- Vendor supplied default passwords must be changed and any unnecessary default accounts removed or disabled before installing a system on the network.

3.3 Asset Security Standards

Additional guidance on Asset Security standards is available in Domain Guideline C: Asset Management.

3.3.1 Hosted IT Service Standards

Hosted services (e.g. cloud computing, Software-as-a-Service, cloud subscriptions services) is a rapidly evolving trend by which the University and its clients procure services through use of cloud (host)-based infrastructure, networking and applications over the internet. In particular:

- The University's information systems may involve the storage of systems/services outside of the University and/or outside of Australia. To the extent that any information system/service contains any confidential or Personal Information (as that term is defined in the Information Privacy Act 2009), that data may be stored outside of the University and/or overseas. While the University will enter into confidentiality arrangements to protect the privacy of such data (including adherence where relevant to the General Data Protection Regulation (GDPR) and Data US-EU Safe Harbour Program), any data stored outside of the University and/or outside of Australia may be subject to compulsory access through process of law, under the relevant jurisdiction in which it is stored
- Any University staff member seeking to deploy or procure such services, as a minimum, must comply with Griffith's Cloud Hosting Policy and:
  - Seek advice from Digital Solutions prior to acquiring or deploying cloud services
  - Conform to the decision-making framework for hosting services
  - Comply with the Solutions Architecture Board (SAB) requirements and the Security Checklist for hosted services
  - Seek University Legal Services and Planning and Financial Services' advice on contracts and agreements
  - Where the service involves storage of staff or student data and/or Enterprise Infrastructure Recurrent Plan (EIRP), obtain approval from the Chief Operating Officer.

3.3.2 Internet and Network Access Security Standards

The following are the minimum accepted standards for protection of Internet capable devices operating on Griffith University network:

- A border router, firewall, or equivalent, will be used with all systems containing content not of a public nature and requiring authenticated connection
- All data packets and connection requests will be controlled by the firewall, or equivalent
- Only explicitly permitted traffic is allowed through the firewall, or equivalent. All other traffic is rejected
- All traffic passing through the firewall must be captured and logged and capable of being audited
- Where possible and practical, traffic passing through the firewall will be capable of being encrypted. Access to content not of a public nature will be encrypted in accordance with current Data Retention Legislation (DRL) plan
- Packet filtering will be used with rules which keep the security risk to a minimum
- All Internet/Web servers which require connectivity to Griffith University network must be approved by the Chief Digital Officer or delegated authority
- All servers being connected to the data centre must be subject to a vulnerability scan to determine security posture and appropriate risk remediation steps identified and

implemented prior to connecting to the Internet; additionally, appropriate firewall rules must be applied at the data centre and Internet level for all connecting servers

- All Internet/Web servers will have non-necessary services disabled based on a risk assessment of required services
- Network equipment including but not limited to Wireless Access Points (WAPs) which have not been authorised to operate in association with the Griffith network will be subject to immediate disconnection or isolation by delegated authority of the Chief Digital Officer
- Devices which are identified as having the potential to cause malicious network activity such as virus infection, ransomware, unauthorised access or data exfiltration will be subject to immediate disconnection or isolation by delegated authority of the Chief Digital Officer
- Staff must take appropriate steps to ensure the security of their devices when operating on non-Griffith networks (such as public, conference, hotel or airport Wi-Fi etc.) by using the Griffith VPN service wherever practical and ensuring that operating systems and anti-virus software is kept updated
- Vendor supplied default passwords must be changed and any unnecessary default accounts removed or disabled before installing a system on the network
- All Internet/Web servers will be configured to allow access to and use of services to be controlled (e.g. Access Control Lists, TCP Wrappers).

3.3.3 Internet of Things (IoT) Security Standards

- All non-Standard Operating Environment (non-SOE) devices and associated systems (i.e. Internet of Things (IoT)) are subject to the same security standards and controls as regular IT systems and services. Both newly introduced IoT as well as architectural changes to existing IoT must comply with the Digital Solution's Security Architecture Board (SAB) and Change Advisory Board (CAB) processes
- If IoT involves use of a cloud service, implementation of the IoT system must comply with the requirements in the Cloud Hosting Policy
- IoT devices which require a network address (allocated via NetReg) must comply with the NetReg minimum baseline security checks
- IoT devices must be subject to a vulnerability scan to determine security posture and appropriate risk remediation steps identified and implemented prior to connecting to the Internet; additionally, devices must be placed in an appropriately segmented network as defined by Griffith Internet of Things (IoT) governance framework.

3.3.4 Email Security Standards

The following are the minimum acceptable standards for the use and management of email within the University's information management and technology environment:

- A password must be used on all email systems
- The use of scanned signatures will be discouraged
- Email communication is not private. Any email that is non-business related should have a disclaimer that the opinions are the individual's and not those of the University
- The University's email system may involve the storage of emails outside of Australia. To the extent that any email contains any confidential or Personal Information (as that term is defined in the Information Privacy Act 2009), that data may be stored overseas. While the University has entered into confidentiality arrangements to protect the privacy of such data (including adherence to the US-EU Safe Harbour Program), any data stored outside Australia may be subject to compulsory access through process of law, under the relevant jurisdiction in which it is stored

- Further guidance on email security standards is available in the Email Security policy.

3.3.5 Social Media Standards

The following principles apply to the use and management of social media within the University's information management and technology environment:

- **Etiquettes** – Social media users should be aware of their responsibilities in regards to categories of social media networks, roles and responsibilities and social media guidance as described in Social Media Guidelines and the Information Technology Code of Practice.
- **Sharing** – Social media users must not share confidential, proprietary, offensive or potentially embarrassing information with others.

3.3.6 Backup and Recovery Standards

The following are the acceptable standards for backup and recovery of the University's information resources:

- Backup cycles to be related to the business risk, frequency with which data and software are changed, and the criticality of the system to business operations
- Any requests by clients for data backup must be done via submission of a *Request to Backup Data* form
- A register of backups, including verification of their success, to be maintained in-line with the compliance requirements
- A cycle of backup media to be used for all backups of corporate systems, the length of cycle is specified in the Request to Backup Data form
- In addition to the above, a system backup to be performed before and after major changes to either the operating system, system software or applications
- In some instances, files may be backed up from one disk to another disk. This would be acceptable if the target disk is not in the same location. If the disks are in the same location, backup of critical data to also be performed to another offsite storage
- Consideration to be taken when upgrading backup technologies to ensure that existing backup data is able to continue to be read
- Regular tests of key corporate systems' backup data to be performed (in a safe environment) to verify that the system can be recovered from the backups produced
- A cycle of backup media to be retained of all information required to meet customer service, legal or statutory obligations
- Operator logs to be maintained, monitored and reviewed on a regular basis to ensure that correct computer operating procedures have been complied with
- Where information is on an externally hosted service, backup by that service provider or backup to customer site must be considered for that service and included within that Service Level Agreement.

3.3.7 Desktop and Mobile Device Timeout and Log Out Standards

With the large number of staff and common use computers and the increasing use of mobile and wireless devices throughout the University, it is essential that unauthorised system access is prevented from these devices.

Where appropriate, device timeouts will be implemented to lockdown the device so that reactivation and access would require entry of a password. Wherever possible, enforced timeouts to be implemented at the following levels:

- Screensaver level
- Page level

- Session level
- Web-based application level

All staff must ensure they activate the screen lockout when they are not physically present at the device they are operating (i.e. when taking a break from their desk, taking lunch, away from work etc.).

All users of common use equipment should ensure they log out of those devices on every occasion to avoid the potential of subsequent users utilising the previously logged-in credentials of the first user to access the internet or web-based applications.

3.3.8 Payment Card Data and Equipment Including EFTPOS Terminals

To ensure compliance with Payment Card Industry (PCI) requirements, the following procedures will be maintained for assets related to payment card data equipment:

- A list of Griffith critical technologies associated with PCI will be maintained, including a list of users and devices which have administrative access to those critical technologies. This will include but not be limited to, any web services and Point of Sale (POS) terminals as part of the PCI environment
- System components and software must be protected from known vulnerabilities by regularly installing applicable vendor-supplied security patches
- Terminal devices should be periodically inspected to look for tampering or substitution of devices
- Sensitive authentication data should not be retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. Payment Account Numbers (PANS) should never be stored in Griffith University network and campus. Not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging
- Payment Account Numbers must be masked when displayed
- PCI media must be disposed of in accordance with media disposal guidelines contained in the related “Guideline C – Asset Management”
- Appropriate levels of network restrictions and user access control must be in place to limit access to equipment, services and information related to payment card data to authorised devices and authorised users only
- A list of service providers that interact with card data must be maintained including a descript
- Authorised devices include all Griffith managed Standard Operating Environment (SOE) devices inclusive of disparate hardware base
- Authorised staff include all Griffith staff who are approved to access related services, information or equipment as part of their role and as approved by their Manager
- Authorised third parties include third parties which Griffith has a formalised agreement within relation to support, development and maintenance of associated equipment and services.

3.4 Operational Security Standards

Additional guidance on Access Control standards is available in Domain Guideline G: Operations Security.

3.4.1 Documentation Operation Procedures

When documenting operating procedures and processes, consideration will be given to the following:

- Where relevant, processes and instructions should be documented in ProMapp to ensure they are identified, captured and recorded for overall business continuity
- User manuals to be maintained on all current hardware, software applications and inhouse developed systems
- Authorisation processes for approving all changes to enterprise information facilities, operating systems, software applications and hardware to be in place
- Procedures to be in place for recording and monitoring of security violations and exposures.

3.4.2 Change Control

To minimise threats to operational environments, consideration will be given to the following:

- Ensuring operational environments are under change control and any changes are subject to the *Request for Change* (RFC) process
- Ensuring adequate testing and change control mechanisms are in place for the migration of new or modified systems into the operational environment
- Ensuring that the information environment is managed so that future expansions or changes can be accommodated and do not adversely impact the operational environment.

3.4.3 Malicious Software

There are many types of malicious software that can severely impact information systems, data and networks and undermine the integrity, confidentiality and availability of information.

To minimise threats to the University's operational environment, consideration will be given to the following activities:

- All operational computer equipment to have the current version of anti-virus software installed and operational
- While server scans are to be run on a regular basis, anti-virus software is to be configured in

  "real-time" mode to ensure any infections are identified and cleaned immediately upon detection
- Anti-virus software to be updated promptly when new definition files become available
- Anti-virus software may not be disabled by staff or students on any Standard Operating Environment (SOE) computer (i.e. managed computers for staff and common use computing areas).

3.4.4 Security Incident Reporting

To minimise the impact of threats and reduce exposure to security incident all suspected and actual security incidents must be reported to the IT Service Centre ithelp@griffith.edu.au. Information on incidents and reporting is available on the Griffith Cyber Security website.

3.4.5 Cyber Security Essentials Training and General Education and Awareness

- Completion of the annual information security awareness training (Cyber Security Essentials Computer Based Training (CBT) course) is mandatory for all Griffith staff
- All staff are responsible to ensure that they, and any of their direct reports complete the CBT on induction and annually
- Education and awareness via regular communication will be sent to users alerting them of potential virus attacks. Users are to be educated about malicious software in general, the risks that it poses, virus symptoms and warning signs including what processes to follow in case of a suspected virus

- Users must be made aware that the installation and use of unauthorised software on University owned assets is prohibited.

3.4.6 Segregation of Duties

There will be adequate separation of functions and duties where tasks involve activities, which could be susceptible to unauthorised activity, misuse of information or pose a conflict of interest.

3.4.7 Operational Environment Separation

Wherever practical, Enterprise information systems development and operational environments will be separated not only logically but physically so that the availability, performance and security of production services are not impacted or compromised. These qualities will also be embraced for systems/services that are externally hosted. Where these types of services are co-located, the relevant University Business Owner will be made aware of associated IT risks.

3.4.8 Software Development Lifecycle

Secure software development lifecycle (SSDLC) control processes will be embedded within the Griffith SDLC process. This will be formally documented within the end-to-end SDLC procedure. Wherever possible, penetration and vulnerability testing should be performed as part of the SDLC process. SSDLC training will be provided to Enterprise Information System (EIS) staff annually or as required.

3.5 Vulnerability and Patch Management Standards

Additional guidance on vulnerability and patch management standards is available in 'Domain Guideline G: Operations Security'.

An established vulnerability and patch management process must be used to regularly monitor for vulnerabilities and patches for information systems. The technical vulnerability management process must be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out when an incident occurs.

The University must deploy a vulnerability management tool to periodically scan the environment for vulnerabilities. The vulnerability management tool must be updated regularly to ensure it is capable of identifying the latest security vulnerabilities.

The Common Vulnerability Scoring Systems (CVSS) will be used where appropriate to rank discovered vulnerabilities according to risk to the environment.

All systems in the University's network environment must have patches applied at the earliest opportunity as per an established patch management regime.

Critical patches must be deployed within one month of the patch's release. Where a critical patch cannot be deployed within one month of release an Information Technology Architecture Board (ITAB) exception must be raised and communicated with the ITAB Chair.

3.6 System Administrator Access Standards

Additional guidance on Access Control standards is available in 'Domain Guideline G: Operations Security'.

Granting of privileged or Administrator level access for production systems to other than specialist system administrators is an exception and comes with responsibility not only for the individual system but the wider health, security and integrity of the University's services, data and reputation.

The University Information Security Procedure places additional obligations on users with privileged or high-level access rights. These staff members are required to abide by the Code of Ethics promulgated

by the System Administrators Guild of Australia (see Appendix A below). System Administrators found guilty of breaching this Code of Ethics may be subject to disciplinary action.

3.5.1 Granting of Administrator Access

i. Principle of Least Privilege

University systems are operated on the principle of least privilege.

The principle means granting a user account only those privileges which are essential to the performance of that user's work. For example, an account used for backing up a system would not be granted privileges to install software.

ii. Alternative to Administrator Access

Most operating systems and applications contain facilities that allow non-Administrator accounts to be granted permission to perform a defined set of functions that would normally require administrator access without granting full administrator access.

Such privileges can be granted for a defined period or on a continuing basis. Examples include the ability to start and stop applications, read system logs, reboot a server and alter application settings. When available these alternatives will be used in preference to administrator access.

iii. Use for Purpose Given

Administrator access is only to be used for purposes for which it was granted. Administrator access does not imply authorisation to undertake activities that are enabled via the privileged access but are not within the purposes for which it was granted.

iv. Process for Granting Administrator Access

A request for administrator access will be submitted to the System Owner for approval. A request can include multiple systems.

The System Owner is the Director, Dean or Head of School/Department of the business area with responsibility for the system.

The request must address:

- Why requirements cannot be achieved by alternatives to administrator access
- The business reasons for access
- Identified risks and mitigations

Approved requests for access will be submitted to Digital Solutions for action.

Requests will be reviewed for IT Security reasons and may be rejected if risks and mitigations are inadequate.

3.5.2 Inappropriate Use of Administrator Access

i. Principle of Least Privilege

In addition to those activities deemed inappropriate in the University Code of Conduct and Information Security Policies, the following constitute inappropriate use of Administrator Access.

Inappropriate use of Administrator Access to University computing resources unless documented and approved by the System Owner includes:

- Circumventing user access controls or any other formal University security controls
- Circumventing bandwidth limits or any other formal University computing controls
- Circumventing formal account activation or suspension procedures
- Circumventing formal account access change request procedures

- Circumventing backup process or other mechanisms designed to ensure the retention and integrity of University data
- Circumventing any other University policy
- Circumventing University change control procedures for IT systems.

Inappropriate use of Administrator Access to University computing resources under any circumstances includes:

- Accessing non-public Information that is outside the scope of specific job responsibilities
- Exposing or otherwise disclosing non-public Information to unauthorized persons
- Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity.

Personal Use is Not Acceptable

- While the University Code of Conduct permits limited personal use of computing resources, this is restricted to **non-administrator** activities.

3.5.3 Administrator Access by Third Parties

Some applications are hosted on University infrastructure and supported by an external third party under contractual arrangements. In a limited number of cases support by the third party requires Administrator access. In addition to the requirements above the following guidelines must be followed.

i. Risks Must be Addressed

The System Owner is responsible for ensuring that the type of data on the system is identified and risks are identified, mitigated and recorded.

Risk areas which must be addressed include but are not limited to:

- Privacy related data in respect of Queensland and Federal Government Privacy Principles and any Privacy Act implications
- Staff, Student and Research data
- Data that has implications for ethics, confidentiality or intellectual property
- Third party access, retention and disposal of data.

If the system interfaces with other University systems, the System Owner must also consider risks to these systems and their data.

Contractual arrangements with the third party should adequately address identified risks.

Risks and mitigations must be registered in the IT risk register and ownership of risk assigned. In addition to those activities deemed inappropriate in the University Code of Conduct and Information Security Policies, the following constitute inappropriate use of Administrator Access.

ii. Access will be via VPN

- All access will be via the University VPN facility
- In accordance with the University security policy, one VPN account per person at the vendor end is required
- For vendors with a large number of support staff, a generic account may be issued.
- When a generic account is provided, vendors must be able to identify on request who utilised the account from their organisation
- VPN password must be changed every six months and must comply with University standards for composition and strength

In the exceptional case where access cannot be achieved via VPN, access will be opened for the duration of the issue or incident only and use only approved access mechanisms.

iii. Access Mechanisms

- All access mechanisms will be via an encrypted service and utilise encryption mechanisms and strengths that match University standards.
- Web-based administration must be via secure HTTP (HTTPS) and utilise a valid SSL certificate of not less than 2048 bits issued by a University certificate authority.
- Webservers and applications will be configured to restrict access to administration services to specific IP addresses or address ranges that will be used to administer systems. Where address ranges are used they should be as narrow as possible.
- Whenever possible administration services should be restricted to internal non-routable addresses.
- Administrator access via unencrypted mechanisms such as telnet and ftp is prohibited.
- Standard supported access mechanisms are SSH over VPN for Unix systems and RDP over VPN for Windows systems.
- Direct login as root to Unix systems is prohibited.
- Third party remote access tools will be considered on a case by case basis. The onus to prove suitability and security of third party tools is on the vendor.
- Vendors are expressly prohibited from providing access to other parties.

iv. External Access Should be Moderated

- Wherever practicable the vendor's administrator account should only be enabled for the duration of required work or investigations and then disabled.

v. Network Controls

- Systems which allow third party administrator access must be built and deployed such that access to other University services and systems is minimised
- An appropriate mix of network controls such as DMZ networks, intrusion detection and firewalls and network ACLS will be used.

vi. Change Control

- Change control will comply with University change control procedures for IT systems. This includes but is not limited to the change management process, authorisation by the Change Advisory Board (CAB) and IT Solutions Architecture Board (SAB) architecture governance processes.

vii. Operating System Configuring and Logging

- The operating system will be deployed, secured and configured in accordance with University standards
- Appliances or prebuilt virtual machines will be assessed by the University security and server support groups for hardening and security
- A copy of operating system and access logs will be made to a system the vendor cannot access. Wherever possible copying will occur in real time
- Operating systems, middleware and applications will be patched in accordance with University requirements specified in the approved standard ‘Guideline G – Operations Security’

- Critical patches must be deployed within one month of the patch's release. Where a critical patch cannot be deployed within one month of release an Information Technology Architecture Board (ITAB) exception must be raised and communicated with the ITAB Chair.

viii. Testing and Vulnerability Assessment Prior to Deployment

- The Cyber Security Team will perform a vulnerability scan of the server or service prior to it going live
- Vulnerabilities will be rectified or mitigated before going live. Where rectification or mitigation is not possible or practicable, a risk must be entered in the University IT risk register.

4.0 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 identities 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.

Digital assets, information and identities 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.

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

APPENDIX 1: CODE OF ETHICS FOR SYSTEM ADMINISTRATORS

Griffith University is a member of The System Administrators Guild of Australia (SAGE-AU).

In a very short period of time computers have become fundamental to the organisation of societies worldwide; they are now entrenched at every level of human communication from government to the most personal. Computer systems today are not simply constructions of hardware -- rather, they are generated out of an intricate interrelationship between administrators, users, employers, other network sites, and the providers of software, hardware, and national and international communication networks.

The demands upon the people who administer these complex systems are wide-ranging. As members of that community of computer managers, and of the System Administrators' Guild of Australia (SAGE-AU), we have compiled a set of principles to clarify some of the ethical obligations and responsibilities undertaken by practitioners of this newly emergent profession.

We intend that this code will emphasise, both to others and to ourselves, that we are professionals who are resolved to uphold our ethical ideals and obligations. We are committed to maintaining the confidentiality and integrity of the computer systems we manage, for the benefit of all of those involved with them.

No single set of rules could apply to the enormous variety of situations and responsibilities that exist: while system administrators must always be guided by their own professional judgement, we hope that consideration of this code will help when difficulties arise.

(In this document, the term "users" refers to all people with authorised access to a computer system, including those such as employers, clients, and system staff.) As a member of SAGE-AU I will be guided by the following principles:

1. Fair Treatment

I will treat everyone fairly. I will not discriminate against anyone on grounds such as age, disability, gender, sexual orientation, religion, race, or national origin.

2. Privacy

I will access private information on computer systems only when it is necessary in the course of my duties. I will maintain the confidentiality of any information to which I may have access. I acknowledge statutory laws governing data privacy such as the Commonwealth Information Privacy Principles.

3. Communication

I will keep users informed about computing matters that may affect them, such as conditions of acceptable use, sharing of common resources, maintenance of security, occurrence of system monitoring, and any relevant legal obligations.

4. System Integrity

I will strive to ensure the integrity of the systems for which I have responsibility, using all appropriate means -- such as regularly maintaining software and hardware; analysing levels of system performance and activity; and, as far as possible, preventing unauthorised use or access.

5. Cooperation

I will cooperate with and support my fellow computing professionals. I acknowledge the community responsibility that is fundamental to the integrity of local, national, and international network resources.

6. Honesty

I will be honest about my competence and will seek help when necessary. When my professional advice is sought, I will be impartial. I will avoid conflicts of interest; if they do arise I will declare them.

7. Education

I will continue to update and enhance my technical knowledge and management skills by training, study, and the sharing of information and experiences with my fellow professionals.

8. Social Responsibility

I will continue to enlarge my understanding of the social and legal issues that arise in computing environments, and I will communicate that understanding to others when appropriate. I will strive to ensure that policies and laws about computer systems are consistent with my ethical principles.

9. Workplace Quality

I will strive to achieve and maintain a safe, healthy, productive workplace for all users.

Procedure

INFORMATION

Printable version (PDF) Downloadable version (Word)

Title	Information Security Procedure
Document number	2020/0000032
Purpose	This document provides mandatory procedures to support the implementation of the Griffith Information Security Policy. It defines the roles and responsibilities of all users, administrators and managers of the University's information technology resources and identifies the standards to be applied ensure security of digital assets, information and associated resources. It also outlines required procedures for operational security management.
Audience	Staff; Students; Public
Category	Operational
Subcategory	Digital Solutions
Effective date	January 2020
Review date	January 2021
Policy advisor	Manager, Cyber Security Governance, Risk and Compliance
Approving authority	Chief Digital Officer

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS

Legislation	N/A
Policy	Information Security Policy Cloud Hosting Policy Compliance Management Framework Griffith University Privacy Plan Information Technology Code of Practice Enterprise Risk Management Framework
Procedures	Data Classification Guidelines Social Media Guidelines
Local protocols	Enterprise Information Systems Standard
Forms	N/A