Information Security Policy Schedule A - Roles, Standards and Operational Procedures

Approving authority	Pro Vice Chancellor (Information Services)
Approval date	3 July 2014
Advisor	Naveen Sharma | Manager, Architecture and Compliance n.sharma@griffith.edu.au | (07) 373 57601
Next scheduled review	2019
Document URL	http://policies.griffith.edu.au/pdf/Information-Security-Policy-Schedule-A-Roles-Standards-Operational-Procedures.pdf
TRIM document	2014/0006761
Description	This document is designed to enable effective implementation of the 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 access & asset control mechanisms for those resources. It also outlines best practice procedures for operational security management.

Related documents

Code of Conduct
Cloud Hosting Policy
Compliance Framework
Enterprise Information Systems Policy
Guidelines on Appropriate Use of Administrative Access to Information Resources
Griffith University Privacy Plan
Information Security Policy
Information Technology Code of Practice
Risk Management Framework
Social Media Guidelines

1. PURPOSE

The purpose of this document is to define the roles and responsibilities of all users of the University's information technology resources and should be read in conjunction with the Information Security Policy.

2. SCOPE

This Schedule applies to all information resources in use by Griffith University. Information technology resources refers to, but is not limited to, information systems that have been developed at Griffith, extended from existing information systems, 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.

3. 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 Chief Technology Officer

The Chief Technology Officer is responsible for:

- Providing specialist information security advice to the Vice Chancellor, Pro Vice Chancellor (Information Services), 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; and
- Implementing disciplinary action for inappropriate use as delegated by the relevant University policies.

3.2 Manager, Architecture and Compliance

The Manager, Architecture 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 Manager, IT Architecture and Compliance's responsibilities include:

- Developing and maintaining the University's Information Security Policy;
- Establishing and maintaining high-level IT security architecture and strategy;
- Coordinating IT Audit activities across Information Services;
- Overseeing the management of the INS IT Risk Register.

3.3 Manager, IT Security

The Manager, IT Security 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, IT Security's responsibilities include:

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

3.4 Business Owners

For each centrally managed administrative system, the Director of a business area 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:

- 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.

3.5 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*.

3.6 Directors, Deans, Heads of School/Department (DDHSD)

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.

3.7 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.

3.8 Information Usage and User Responsibilities

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; and
- 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.

4. ACCESS CONTROL STANDARDS

4.1 Identification Standards

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. 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.
- User IDs and passwords are not to be shared. Users are responsible for maintaining the security of their IDs and all activity occurring under those IDs;
- Accounts designed for use by more than one person are not normally permitted. Exceptions to this can only be authorised by the Chief Technology Officer or delegated authority;
- Guest login accounts are not normally permitted. Guest login accounts can only be issued with the approval of the Chief Technology Officer, Head of Element or delegated authority, as a temporary account;
- 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.

4.2 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;
- In the event of a policy breach, approval to allow access to an account by persons other than the authorised account holder, must be approved by the Chief Technology Officer (or delegate) 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 Technology Officer (or delegate) 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 Technology Officer will authorise proactive vulnerability risk assessment and scanning of the IT infrastructure to improve the University's security posture;
- The relevant Business Owner or Chief Technology Officer (or delegate) 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;
  - The account is used for non-approved activities.

4.3 Authentication Standards

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

- Passwords or approved certificates must be used for accessing all corporate systems;
- 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);
- 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 six months;
- 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 three, 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 the Manager, IT Security.
- 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 Technology Officer (or delegate) and logged in the IT Risk Register..

5. ASSET SECURITY STANDARDS

5.1 Hosted IT Service Standards

Hosted services (e.g. Cloud computing, Software-as-a-Service) is an emerging trend in the manner by which the University and its clients may 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 to the 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; and
- 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 Information Services;
  - Conform to the decision-making framework for hosting services;
  - Comply with the Security Checklist for hosted services;
  - Seek University Legal Services and Planning and Financial Services' advice on contracts and agreements;
  - Where service involves storage of staff or student data, obtain approval from the Vice President (Corporate Services);
  - Where the service involves sensitive research data, obtain approval from Senior Deputy Vice Chancellor.

5.2 Internet 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;
- 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 Technology Officer or delegate;
- All Internet/Web servers will have non-necessary services disabled;
- 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); and
- Use will only be for University-related and approved purposes.

5.3 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.

5.4 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 as described in the Information Technology Code of Practice.
- **Sharing** – Social media users must not share confidential, proprietary, offensive or potentially embarrassing information with others.
- **Attachments** – Social media applications can become channels for malware distribution, so the posting of attachments is discouraged.

5.5 Backup and Recovery Standards

The following are the minimum 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, with at least one copy of each cycle stored off-site; 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 other portable media (such as tape) for 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.
- Data and information stored on the local drive of a computer is not automatically backed up. Backup of these devices is the responsibility of the users.

5.6 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 re-activation 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

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.

6. OPERATIONAL SECURITY PROCEDURES

6.1 Documentation Operating Procedures

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

- User manuals to be maintained on all current hardware, software applications and in-house 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.

6.2 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.

6.3 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:

6.3.1 Virus Detection and Scanning

- All operational computer equipment to have the current version of anti-virus software installed and operational;
- While server scans to be run on a regular basis, anti-virus software 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 to be regularly reviewed, as it may be necessary to use more than one type of scanning software to ensure that maximum protection is provided for all information platforms and environments.

6.3.2 Education and Awareness

- Regular communication will be sent to users alerting them of potential virus attacks. Users 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.

6.4 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.

6.5 Operational Environment Separation

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.

6.6 Software Development Life Cycle

Secure software development lifecycle (SSDLC) control process should be embedded within the Griffith SDLC process. This should 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.

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.