ICT Information Management and Security Policy

1 Purpose

To ensure that Information Security measures are in place, commensurate with their Information Asset classification, to protect Information Assets, Information and Communication Technology (ICT) Assets and Information Systems within the University ICT environment against unauthorised use or accidental modification, loss or release; and assist the University mitigate any damage or liability arising from the use of these Information Assets and Information Systems for purposes contrary to the University's policies and relevant Regulatory Compliance Instrument.

2 Scope

This policy applies to all Employees, Research Workers, University Members and Students (hereafter referred to as 'users') who have access to the University's Information Assets and related Information Systems.

3 Policy Statement

The University is committed to the management of risks associated with ICT Assets and Information Systems and the reduction of ICT security incidents. This policy provides the governance framework for Information management and security within the University and defines the University policy in all aspects of Information Security as stipulated under the relevant Information standards.

4 Principles

4.1 Internal governance

Information Security governance arrangements are established and endorsed by the University ICT Strategy Board and assisted by other relevant University committees. The implementation, maintenance and control of operational Information Security is the responsibility of ICT Services. The ICT Security Committee is responsible for monitoring and recommending Information Security strategy, controls and associated operational security matters.

All Information System users are responsible for familiarising themselves with this policy and related policies and procedures, as appropriate to their role within the University. Effective communication of this ICT Information Management and Security Policy, and all associated policies and procedures, form part of this ongoing commitment to Information Security governance and is critical to ensuring that ICT Assets and Information Assets are protected

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

from unauthorised use, accidental modification, loss or release.

In the event of a cyber breach such as, but not limited to, malware, computer hacking, ransomware, or denial of service attack, the Executive Director (ICT Services) is authorised to implement a range of measures, including removal of individual access to the network and removal of ICT Assets and ICT Systems from the network to minimise the risk of loss or misuse of Information Assets.

4.2 External party governance

The Executive Director (ICT Services) is delegated with ensuring that appropriate arrangements are established and documented to ensure that third party ICT service level agreements, operational level agreements, hosting agreements or similar contracts clearly articulate the level of security required and are regularly monitored.

4.3 Information Security and Cyber Security

Information Security activities, including Cyber Security awareness, are concerned with the protection of Information from unauthorised use or accidental modification, loss or release. Information Security is based on the following five elements:

- **Confidentiality** - ensuring that Information is only accessible to those with authorised access
- **Integrity** - safeguarding the accuracy and completeness of Information and processing methods
- **Availability** - ensuring that authorised users have access to Information when required
- **Compliant Use** - ensuring that the University meets all Regulatory Compliance Instruments and contractual obligations
- **Responsible Use** - ensuring that appropriate controls are in place so that users have access to accurate, relevant and timely Information but that users of the University's ICT resources do not adversely affect other users or other Information Systems.

4.4 Policy, planning and governance

The University recognises the importance of, and demonstrates a commitment to, maintaining a robust University Information Security environment. The University at a minimum will reasonably:

1. develop and implement an Information Security policy (this policy)

2. develop and implement an Information Security Plan, ensuring alignment with the University business planning, general security plan and risk assessment findings

3. establish and document Information Security internal governance arrangements (including roles and responsibilities) to implement, maintain and control operational Information Security within the University. Relevant information shall be provided as needed including provision of timely and relevant information to the University's senior executive and Council regarding Information Security matters.

4. establish, document and regularly monitor Information Security external governance arrangements to ensure that third party service level agreements and operational level agreements clearly articulate the level of security required.

4.5 Recordkeeping and Information Privacy

For the purposes of the University's records management System and Information management, the University is required to comply with multiple Regulatory Compliance Instruments, including but not limited to:

- *Information Privacy Act 2009*
- *Public Records Act 2002*
- Records Governance Policy
- Queensland Information Standard 18: Security.

The University will meet its data retention obligations under the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (section 187) recognising that the University will rely on the 'immediate circle' exclusion for any relevant services provided only to persons who are 'inherently connected to the functions of the University'.

4.6 Information Asset management

The University has developed the Information Asset and Security Classification Procedure which establishes the process for classifying and handling University Information Assets based on their level of sensitivity, value and criticality to the University.

4.7 People Portfolio management

The University will implement measures to minimise the risk of loss or misuse of Information Assets by ensuring that Security Safeguards are incorporated into University People Portfolio management, including the development of supporting policies and processes. The University at a minimum will reasonably:

1. implement induction and ongoing training and security awareness programs to ensure that all Employees are aware of and acknowledge this policy and related policies and procedures on Information Security and security responsibilities

2. document and assign security roles and responsibilities where Employees have access to security classified Information or perform specific security related roles, and ensure that security requirements are addressed in recruitment and selection and in job descriptions

3. develop and implement procedures for the separation of Employees from, or relocation within, the University.

4.8 Physical and environmental management

The University will apply measures to ensure that the level of physical controls implemented will minimise or remove the risk of equipment or Information being rendered inoperable or inaccessible, or being accessed, used or removed without authorisation. The University at a minimum will reasonably ensure that:

1. building and entry controls for areas used in the processing and storage of security classified ICT Information are established and maintained, consistent with the Information Asset and Security Classification Procedure

2. all ICT Assets that store or process Information are located in Secure Areas with control mechanisms in place to restrict access to authorised personnel only

3. Policies, procedures and processes are implemented to monitor and protect the use and/or maintenance of Information Assets and mobile ICT Assets away from University premises

4. Policies, procedures and processes are implemented for the secure disposal or reuse of ICT Assets, commensurate with the Information Asset's security classification level.

4.9 Communications and operations management

The University will ensure that operational procedures and controls are documented and implemented to ensure that all Information Assets and ICT Assets are managed securely and consistently, in accordance with the level of required security. The University at a minimum will reasonably ensure that:

1. operational change control procedures and release management control procedures are implemented to ensure that changes to Information processing facilities or Systems are appropriately approved and managed

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

2. System capacity is regularly monitored to ensure risks of System overload or failure, which could lead to a security breach, are avoided

3. adequate controls are defined and implemented to mitigate the impact of threats and vulnerabilities to the network, including the prevention, detection, removal and reporting of attacks of malicious code on all ICT Assets

4. Systems maintenance processes and procedures, including operator and audit/ fault logs, media handling procedures, Information backup procedures and archiving, will be implemented

5. methods for exchanging Information within the University, outside the University, through online services, and/or with third parties, will be consistent with the Queensland Government Information Security Classification Framework (QGISCF) and the Network Transmission Security Assurance Framework (NTSAF) and University policies and procedures

6. confidentiality requirements or non-disclosure agreements reflecting the need for protecting Information are to be undertaken in accordance with the University's Intellectual Property Policy and related procedures and identified and reviewed regularly

7. each Employee must use the University authorised and supplied communications methods, including electronic mail, when transacting official University business.

8. the Student Communication Policy and related policies and procedures cover Handling Personal Student Information Policy and Procedure, Student Communication Procedure, Use of Electronic Mail Procedure establish the framework for all electronic communications with Students.

4.10 Access management and passwords

The University will put in place control mechanisms based on business requirements, assessed/accepted risks, Information classification and Regulatory Compliance Obligations for controlling access to all Information Assets and ICT Assets. The University at a minimum will reasonably ensure that:

1. access will be provided to users for the purpose of carrying out work, study or other activities as agreed with the University

2. access will be granted on the 'least privilege' principle in which each user is granted the most restricted set of privileges needed for the performance of the relevant tasks

3. authentication requirements, including on-line transactions and services, must be appropriate for the security classification of the Information

4. access to the University network and Information Systems requires specific authorisation

and each user must be assigned an individually unique personal identification code and secure means of authentication

5. access to shared ICT Assets in teaching and research laboratories may be subject to shared access management rules as agreed by the University

6. policies and/or procedures for user registration, authentication management, access rights and privileges are defined, documented and implemented for all ICT Assets

7. 'restricted access' and 'authorised use only' warnings must be displayed upon access to all Systems which have this capability.

There is an obligation on Employees who are studying University Courses, who also have a level of administration access to related University Systems, to contact the Course Examiner for the Course/s the Employee is studying to alert them to this fact. This also applies to Employees with relationships to Students studying University Courses resulting in a perceived, potential or actual conflict of interest, as identified in the Employee Conflict of Interest Procedure. During the course of their study, the Employee is not permitted to access the relevant Course environments, or applicable Systems, using their administrator access.

The University requires users to keep user-level passwords confidential and change these immediately if they suspect that their password has been comprised.

A Clear Desk and Clear Screen is required to reduce the risk of unauthorised access or damage to Information Assets and ICT Assets.

4.11 System acquisition, development and maintenance

The University will apply measures to ensure that during System acquisition, development and maintenance, Security Safeguards will be established and will be commensurate with the security classifications of the Information contained within, or passing across, Information Systems, network infrastructure and applications. The University at a minimum will reasonably ensure that:

1. security requirements are addressed in the specifications, analysis and/or design phases and internal and/or external audit are consulted when implementing new or significant changes to financial or critical business Information Systems

2. Security Safeguards are established during all stages of System development, as well as when new Systems are implemented and maintained in the operational environment

3. appropriate change control, acceptance and System testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment

4. a patch management program for operating Systems, firmware and applications of all ICT Assets is implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited.

4.12 Incident management

The University will ensure the effective management of and response to Information Security incidents to maintain secure operations within the University. The University at a minimum will reasonably:

1. establish and maintain an Information Security incident and response register and record all incidents

2. ensure all Information Security incidents are reported and escalated (where applicable) through appropriate management channels and/or authorities

3. ensure that incidents are investigated and apply formal disciplinary processes

4. ensure responsibilities and procedures for the timely reporting of security events and incidents, including breaches, threats and security weaknesses, are communicated to all University Members.

4.13 Business continuity management

The University will ensure that a managed process, including documented plans, is in place to enable Information and ICT Assets to be restored or recovered in the event of a disaster or major security failure. The University at a minimum will reasonably:

1. establish plans and processes to assess the risk and impact of the loss of Information and ICT Assets on University business in the event of a disaster or security failure and develop methods for reducing known risks to University Information and ICT Assets

2. ensure business continuity Information and ICT Asset disaster recovery plans are maintained and tested to ensure Systems and Information are available and consistent with agency business and service level requirements.

University Members should also refer to the Business Continuity Policy and Crisis Management Policy (under development).

4.14 Compliance management

The University will implement practices to ensure compliance with, and appropriate

management of, all Regulatory Compliance Instruments relating to Information Security. The University at a minimum will reasonably ensure that:

1. all Information Security policies, procedures and processes, including contracts with ICT third parties, are reviewed for compliance on a regular basis

2. all reporting obligations relating to ICT Security are complied with and managed appropriately

3. all reasonable steps are taken to monitor, review and audit University Information Security compliance, including the engagement of internal and/or external auditors and specialist organisations where required.

University Members should also refer to the Policy and Procedure Framework.

4.15 Penalties and discipline

Conduct in contravention of this policy may constitute a criminal offence under relevant State and Commonwealth legislation, resulting in legal prosecution. Where the violation is considered a criminal offence, the police (Federal and State) will be informed. Where applicable, the Director (Integrity and Professional Conduct) will also be advised.

This will be irrespective of whether the violation is internal (e.g. unauthorised access to Information), external (e.g. unauthorised remote access to the University network by a non-University Employee or Student), or where assistance is provided by a University Employee or Student to provide unauthorised access to the University network.

4.16 Other considerations

The University will make no warranty, explicit or implied, regarding the ICT services offered, nor their fitness for any particular purpose. Similarly, no responsibility can be accepted by the University or its Employees, for any damage arising directly or indirectly from the use of these services.

The responsibility for protecting ICT resources and services is shared with all users who use these services. The University will make all reasonable efforts to protect University Members from possible ICT and computer-related dangers but cannot always protect University Members from all potential threats. The University cannot guarantee to protect an individual against exposure to material that may be offensive to them. University Members will be warned that they may traverse or receive material that they find offensive.

5 References

Australian Government. (2015). *Telecommunications (Interception and Access) Amendment*

(Data Retention) Act 2015. Canberra, Australia: Australian Government Retrieved October 13, 2016 from https://www.comlaw.gov.au/Details/C2015A00039.

Queensland Government Chief Information Office (Policy, Enterprise Architecture and Security). (2013). *Queensland Government Network Transmission Security Assurance Framework (NTSAF).* Retrieved November 6, 2013, from https://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2401-network-transmission-security-assurance-framework

ICT Policy and Coordination Office. (2010). Queensland Government Authentication Framework (QGAF). Retrieved November 6, 2013, from http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2415-queensland-government-authentication-framework

Queensland Government Chief Information Office (Enterprise Architecture and Strategy). (2009). *Queensland Government Enterprise Architecture Framework 2.0.* Retrieved November 6 2013, from https://www.qgcio.qld.gov.au/products/qgea-documents/547-business/2786-queensland-government-enterprise-architecture

Queensland Government Chief Information Office. (2013). *Queensland Government Information Security Classification Framework (QGISCF)*. Retrieved November 6, 2103, from http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2417-queensland-government-information-security-classification-framework

6 Schedules

This policy must be read in conjunction with its subordinate schedules as provided in the table below.

7 Policy Information

Accountable Officer	Deputy Vice-Chancellor (Enterprise Services)
Responsible Officer	Deputy Vice-Chancellor (Enterprise Services)
Policy Type	Executive Policy
Policy Suite	Cloud Computing Use Inherent Risk Schedule Engagement of Cloud Computing Services Procedure
Subordinate Schedules	
Approved Date	20/10/2017
Effective Date	20/10/2017
Review Date	18/7/2020

Relevant Legislation	ISO/IEC 27000:2016 - Information technology - Security techniques - Information security management systems - Overview and vocabulary AS ISO/IEC 27001:2015 - Information technology - Security techniques - Information security management systems - Requirements AS ISO/IEC 27002:2015 - Information technology - Security techniques - Code of practice for information security controls AS/NZS ISO/IEC 27005:2012 - Information technology - Security techniques - Information security risk management *Electronic Transactions (Queensland) Act 2001* *Information Privacy Act 2009* Information Security Manual - ISM (Australian Government) Metadata Management Principles Network Transmission Security Assurance Framework *Public Records Act 2002* *Public Sector Ethics Act 1994* Queensland Government Information Security Classification Framework Queensland Information Standard 13: ICT Procurement and Disposal of ICT Products and Services Queensland Information Standard 18: Information Security Queensland Information Standard 26: Internet Queensland Information Standard 31: Retention and Disposal of Public Records Queensland Information Standard 44: Information Asset Custodianship Records Governance Policy *Right to Information Act 2009* *Telecommunications (Interception and Access) Amendment (Data*

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

	Retention) Act 2015 *University of Southern Queensland Act 1998*
Related Policies	Acceptable use of ICT Resources Policy Business Continuity Policy Code of Conduct Policy Contract Management Policy (under development) Crisis Management Policy (under development) Employee Complaints and Grievances Policy Enterprise Architecture Policy Handling Personal Student Information Policy and Procedure Institutional Planning Policy and Procedure Intellectual Property Policy and Procedure Mobile Device and Service Policy Official Information Policy and Procedure Physical Security Policy (under development) Policy and Procedure Framework Privacy Policy Procurement Policy Public Interest Disclosure Policy Quality Management Framework Records and Information Management Policy Research Code of Conduct Policy Risk Management Policy and Procedure Student Code of Conduct Policy

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

	Student Communication Policy Under 18 International Students Policy
Related Procedures	Contract Management Procedure (under development) Crisis Management Procedure (under development) Electronic Access Control Procedure Employee Conflict of Interest Procedure Information Asset and Security Classification Procedure Key Control Procedure Records and Information Management Procedure Recruitment and Selection Procedure Student Communication Procedure Student General Misconduct Procedure Use of Electronic Mail Procedure
Related forms, publications and websites	Enterprise Information Management Framework (EIM Framework) Use of copyright materials guideline
Definitions	**Terms defined in the Definitions Dictionary**
	Council Council means the governing body, the University of Southern Queensland Council. Course A discrete element of a program, normally undertaken over a single Teaching Period, in which the Student enrols, and on completion of which the Student is awarded a grade. Employee A person employed by the University and whose conditions of employment are covered by the USQ Enterprise Agreement and includes persons employed on a continuing, fixed term or casual basis. Employees also include senior Employees whose conditions of

employment are covered by a written agreement or contract with the University.

Examiner

A University staff member, normally an academic staff member, continuing or fixed term, appointed to be responsible for the conduct and Assessment of a Course in accordance with the prescribed Course Specification.

General Misconduct

Behaviour or conduct by a Student which: is deemed to be serious in nature; and is a deliberate failure to comply with the specific provisions of the Student Code of Conduct; and/or is persistent or negligent behaviour in breach of the Student Code of Conduct; and does not constitute as Academic or Research Misconduct, including a breach in research or failure to implement the Research Code of Conduct.

Information

Any collection of data that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.

Information Asset

An identifiable collection of data stored in any form and recognised as having value for the purpose of enabling the University to perform its business functions, thereby satisfying a recognised University requirement.

Information Security

Concerned with the protection of Information from unauthorised use or accidental modification, loss or release.

Information System Custodian

An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a System within the University.

Information Systems

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

	The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information. Regulatory Compliance Instrument An external compliance instrument provided by legislation, regulation, standards, statutes or rules, including subordinate instruments. Regulatory Compliance Obligation An external obligation provided in Regulatory Compliance Instruments. Research Worker Any person/s involved in Research Activities at, or on behalf of the University. This includes, but is not limited to Employees, Students, visiting scholars, research partners, research affiliates, holders of Honorary or Adjunct positions and research ethics committee members. Student A person who is admitted to an Award Program or Non-Award Program offered by the University and is: currently enrolled in one or more Courses or study units; or not currently enrolled but is on an approved Leave of Absence or whose admission has not been cancelled. University The term 'University' or 'USQ' means the University of Southern Queensland. University Members Employees of the University whose conditions of employment are covered by the USQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; Members of the University Council and University Committees; Visiting and adjunct academics; Volunteers who contribute to University activities or who act on behalf of the University; Individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors and consultants, where applicable.

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

Definitions that relate to this policy only

Clear Desk

Clear desks at the end of each work day of all sensitive Information Assets including documents and notes, business cards, and removable media (e.g. USB memory sticks) to ensure a reduction of the risk of information theft, fraud, or a security breach caused by sensitive Information being left unattended and visible in plain view.

Clear Screen

Locking computers when leaving a desk unattended and logging off when leaving for an extended period of time to ensure that the contents of the computer screen are protected from prying eyes and the computer is protected from unauthorised use.

Cyber Security

Measures relating to the confidentiality, availability and integrity of Information that is processed, stored and communicated by electronic or similar means.

Source: Australian Government. (2016). Attorney-General's Department - Cyber security. Retrieved from https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx

ICT Asset

All applications and technologies that are owned, procured and/or managed by the University. These include desktop and productivity tools, application environments, hardware devices and Systems software, network and computer accommodation, and management and control tools.

Public Record

Refer Section 6 *Public Records Act 2002*.

A public record is any form of recorded Information that provides evidence of the decisions or actions of a 'public authority' (in this case the University of Southern Queensland) in undertaking its business activities or in the conduct of its affairs. The Act includes all records (and Information) irrespective of the form, the custodial arrangements and the technology used to generate, manage, preserve and access records.

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.

	Secure Area Provides the highest integrity of access to, and audit of, Security Classified Information Assets to ensure restricted distribution and to assist in subsequent investigation if there is unauthorised disclosure or loss of Information Assets. The essential physical security features of a Secure Area include, but are not limited to: • appropriately secured points of entry and other openings • tamper-evident barriers, highly resistant to covert entry • an effective means of providing access control during both operational and non?operational hours • all persons to wear passes • all visitors escorted at all times • during non-operational hours a monitored security alarm system, providing coverage for all areas where Security Classified Information Assets are stored • an approved means of limiting entry to authorised persons. **Security Safeguards** Hardware, programs, procedures, policies and physical safeguards which are put in place to assure the integrity and protection of an Information Asset System together with other forms of control including training. **System** A combination of Information Assets and ICT Assets supporting a business process.
Keywords	Information management and security
Record No	13/340PL

Complying with the law and observing Policy and Procedure is a condition of working and/or studying at the University. A hard copy of this electronic document is uncontrolled and may not be current as the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the University's Policy and Procedure Library.