ICT Security - Operational Policy

1. Purpose of policy

This policy outlines the commitment of the University to effectively managing the security risks to Information and Communication Technology (ICT) assets and the obligations of the University community in protecting these resources.

The policy is consistent with the Queensland Government's Information Standard IS18 and the ISO/IEC 27001 standard.

2. Policy scope and application

This policy applies to all staff, students and other members of the University community who may access and use the University's ICT Assets.

3. Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to this policy and are critical to its effectiveness:

Business System Owner means the nominated custodian that has responsibility for the security of the data and application component of the ICT Asset and is also accountable for those aspects of the Information System. Business System Owners for each of the University's Information Systems are identified in the Schedule: Information Systems Owners and Classification.

Cost Centre Manager means the most senior officer or member of staff responsible for the management of a School or a management or support service or administrative area or sub-section of which that is specifically identified for allocation of funding within the University's budget framework.

End-User Developed Information System means an Information System developed by an individual(s) outside the University's IT development guidelines (e.g. an Excel Spreadsheet or Access database).

Information and Communication Technology (ICT) Asset means all software, hardware and data used in the management of the related University information resources. (Note: This may include non-ICT resources (e.g. Printed records))

Information Classification means the categorisation of an ICT Asset for the purposes of identifying the security controls required to protect that asset (see section 5.1, below).

Information System means an electronic system that manages information and data related to the ICT Asset.

Information Security Management System means a collection of artefacts that support the ICT Security Policy framework, consistent with the Queensland Government's Information Standard IS18 and the ISO/IEC 27001 standard.

Segregation of Duties means a separation of responsibilities in undertaking a task to minimise the likelihood of compromising security.

Third Party University Clients means contractors, consultants, adjunct appointments and other individuals who are not University staff or students but who require access to University Information Systems.

University Clients means staff and students of the University as well as Third Party University Clients.

4. Policy Statement

4.1 The University is committed to the operation of a policy framework that supports the secure management of ICT assets and the reduction of ICT security incidents that impact on the confidentiality, integrity and availability of information housed in the University's Information Systems.

4.2 Business System Owners, acting as custodians of business systems and the Information Technology department have shared responsibilities for ensuring that the University's Information Systems are secure and remain compliant with this Policy. These responsibilities are identified within the Information Systems Operations – Procedures.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Director, Information Technology

FIRST APPROVED

8 December 2007

LAST AMENDED

11 January 2019

REVIEW DATE

8 August 2022

STATUS

Active

4.3 University Clients are provided access to University's ICT assets in accordance with the Information and Communications Technology (ICT) Access Control – Managerial Policy and are expected to use this access in accordance with the Acceptable Use of Information Technology Resources - Governing Policy. University Clients are responsible for protecting their means of accessing University ICT assets (e.g. login & password, ID card), not compromising the security of ICT assets and maintaining security over the information they access and use.

5. Information system classification

5.1 Each Information System will require its own level of security based on its Information Classification. The University classifies Information Systems in accordance with the Information Asset Security Classifications and Handling – Guidelines (available for staff access on MyUniSC).

6. Physical and system access control

6.1 Physical access controls for the University premises will be implemented in accordance with the risk and the importance of the ICT Asset to be protected. Unattended access equipment (e.g. PC) is to be protected through physical or electronic means (e.g. System timeout).

6.2 Access to Information Systems at the University is to be provided to University Clients for the purpose of carrying out work, study or other activities as agreed with the University and as appropriate to the client's role.

6.3 Security risks should be assessed and managed in relation to the physical location of an ICT Asset, particularly where this location is offsite from University premises.

6.4 Appropriate control mechanisms (e.g. Username and password) will be in place for authenticating access to all non-Public Information Systems and appropriate ICT Assets. Access control must be in accordance with the Information Classification.

6.5 Access granted to Third Party University Clients is to take into account the risks involved, with adequate controls put in place to protect the University's ICT Assets (e.g. the most limited access rights in the system as possible in order to carry out the work). In addition, the Business System Owner may require Third Party University Clients to sign a University confidentiality agreement.

6.6 In assessing risks to Information Systems, the Business Systems Owner must consider the security of the information in all media formats that will be used (e.g. hardcopy). Furthermore, consideration is required when information may be stored on mobile equipment which can be transported offsite (such as laptops, USB sticks and mobile phones). The Information Technology department will provide solutions to lock access to mobile media on individual systems where practical.

6.7 Remote access to Restricted Information Systems will only be provided by the Information Technology department with the explicit authorisation of the Business System Owner.

6.8 Ownership of information, data and software within the University is assigned in a manner consistent with the University's Intellectual Property – Governing Policy or with other contracts and agreements.

6.9 University Clients are required to access and use the University's ICT Assets in accordance with the Acceptable Use of Information Technology Resources – Governing Policy.

7. Operations management

7.1 Operations management procedures in relation to this policy will be maintained in the Information System Operations – Procedures and within the Information Security Management System.

7.2 Changes to Information Systems will be subject to formal testing and change control procedures.

7.3 To reduce risk in the use of Information Systems, the Business System Owner (with consultation from the Information Technology department) should ensure that there is an appropriate segregation of duties. The Information Technology department will advise Business System Owners on effective segregation of duties, having regard to industry good practice.

7.4 The Information Technology department will ensure that appropriate systems will be in place to facilitate the detection and prevention of malicious software into the University's ICT environment (e.g. The use of anti-virus software).

7.5 The installation of unauthorised information and communications technology on the campus network is prohibited (e.g. installation of hardware or network software; physical interference with hardware, network connections, or cabling, etc.).

7.6 Backup for practices will be in place for all Business Systems. Backup media will be protected in an alternate location to the Information System. Operations, support and maintenance of backups and backup regimes are the responsibility of the Information Technology department, after consultation from Business System Owners with confirmation of items to be backed up.

7.7 Appropriate activity logging will be in place for all Business Systems.

7.8 ICT Security incidents will be dealt with in a manner consistent with the University's Critical Incident Management – Managerial Policy.

7.9 Restricted information is only to be transmitted across any accessible part of the network in a secure manner (preferably using encryption). The Information Technology department will provide the means and/or training for users to be able to do this.

7.10 Business continuity is to be managed in accordance with the University's Business Continuity Management – Managerial Policy.

8. Information system development and maintenance

8.1 Business Systems will be developed in accordance with the Application Development Guide.

8.2 ICT security requirements will be addressed wherever possible as part of the acquisition, implementation or development of the Business System.

8.3 Cost Centre Managers must ensure that any Information System developed for their area has adequate security features and these will be implemented to the satisfaction of any internal or external audit review. The development of these controls may require liaison and/or support with the Information Technology department and other Cost Centres.

8.4 Where business continuity is critical, End-User Developed Information Systems will be avoided, or will be institutionalised and brought under the management of the Information Technology department where critical to ongoing operations.

9. Compliance

9.1 The University monitors and logs activity on its ICT Assets and Business Systems and carries out security audits on these systems as required. The University reserves the right to access individual files.

9.2 The security of the University's ICT Assets and Business Systems will be audited periodically and reported to appropriate University committees.

9.3 Breaches of this policy shall be treated as misconduct or serious misconduct and will be dealt with under relevant University policies including the Staff Code of Conduct - Governing Policy, and the Student Conduct - Governing Policy. The University reserves the right to restrict access by an individual to ICT Assets when faced with evidence of a breach of University policies or law. Breaches that violate State or Commonwealth law shall be reported to the appropriate authorities.

10. Authorities/Responsibilities

The following authorities are delegated under this policy:

ACTIVITY	UNIVERSITY OFFICER
Uniquely identified and assigned a Business System Owner for each Business Systems.	Chief Operating Officer
Assessment of assigned Business System for its Information Classification in consultation with Information Management Services. Business System Owners are responsible for overseeing their assigned Business System in accordance with this policy and associated procedures.	Business System Owner
Monitoring the University's ICT network infrastructure, including all hardware and communications links, and addressing any audit issues that may be identified in relation to these items.	Director, Information Technology
Monitoring their Business System, authorising and revoking access and addressing any audit issues that may be identified, with the assistance of the Information Technology department.	Business System Owners
Avoidance of breaches of legal, statutory, regulatory, contract or privacy obligations, through: • Monitoring of compliance obligations for the University's ICT network infrastructure; • Assisting Business System Owners in monitoring compliance for the University's Business Systems; and • Assisting with internal and/or external audits, including reporting on the status of audit issues.	Director, Information Technology
Ensuring that a central authentication system (such as usernames and passwords) is available and provides secure access by University Clients to Business Systems classified as Internal.	Director, Information Technology
Maintaining an Information Security Management System in support of this Policy.	Director, Information Technology
Ensure that staff are trained in the effective use of their assigned Business System.	Business System Owners

Schedule A: Business Systems, Owners and Classification

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Governing Policy

- Acceptable Use of ICT Resources - Procedures
- Adopting Cloud-based Services - Procedures
- Business Continuity Management - Governing Policy
- Compliance Management Framework - Governing Policy
- Compliance Management Framework - Procedures
- Critical Incident Management - Governing Policy
- ICT Access Control - Operational Policy
- Incident Management - Procedures
- Information and Records Management - Procedures
- Information Management - Governing Policy
- Information System Operations - Procedures
- Intellectual Property - Governing Policy
- Intellectual Property: Commercialisation - Procedures
- Intellectual Property: Commercialisation Revenue - Procedures
- Intellectual Property: Student IP - Procedures
- Intellectual Property: Transfer of Rights to Creators - Procedures
- Resolution of Complaints (Staff) - Guidelines
- Risk Management - Governing Policy
- Staff Code of Conduct - Governing Policy
- Student Conduct - Governing Policy

RELATED LEGISLATION / STANDARDS

- Queensland Information Standards