

(Standard) ICT Standard for Human Resources Security

Document Purpose

Document Purpose	This standard defines the ICT Human Resource Security Management strategies and processes implemented by the University.			
Document Information	Version	1.0		
	Release Date	November 2009		
	Release Status	Final		
	Review Date	November 2010		
	Author(s)	Principal Manager - PMIM		
	Owner	Principal Manager - PMIM		
	Print Date	Last Printed: 21/06/2010 12:22:00 PM		
	Approved By	Principal Manager - PMIM		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/resources/ict_standard_for_human_resources_security.pdf		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2008	Various	Document creation
	1.0	July 2008	Maggie Fryer	Final release
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

- Document Purpose 1**
- Document Information 1**
- Error Advisory 1**
- 1 Definitions 3**
- 2 Introduction 3**
- 3 Standards 4**
 - 3.1 Information Security Education and Training 4
 - 3.2 Client Training 4
 - 3.3 Security in Job Descriptions 4
 - 3.4 Outsourcing and Third-Party Access 5
 - 3.5 Separation Processes and Movement within the University 6
 - 3.6 Confidentiality Agreement 6
 - 3.7 Reporting Incidents and Violations 6
 - 3.8 Offsite Use of ICT Resources and Mobile Computing 7
 - 3.9 Disciplinary Process 7
- 4 Related Documents 8**

1 Definitions

The *ICT Glossary and Definitions* contains a description of any common ICT terminology referred to in the policy and standard documentation.

2 Introduction

The University will implement a range of strategies and processes to minimise the risk of loss or misuse of information assets by ensuring that security controls are incorporated into University ICT human resource management. These include a commitment by the University to:

- Implement induction programs and continually assess and improve the level of ongoing training and security awareness programs, to ensure that clients, including staff and student, are aware of and acknowledge their security responsibilities and that clients are provided with the appropriate skills for the correct use of University ICT resources;
- Document security roles and responsibilities where staff 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;
- Develop and implement procedures for the separation of staff from, or movement within, the University;
- Communicate responsibilities and procedures to all clients including staff, students, contractors and third parties for the timely reporting of security incidents including breaches, threats and security weaknesses;
- Ensure that security violations or breaches are investigated and where it is found that a deliberate violation or breach has occurred, that formal disciplinary processes are applied; and
- Ensure that security measures with respect to offsite use of ICT resources are considered and appropriate measures implemented to protect the range of USQ ICT resources.

3 Standards

3.1 Information Security Education and Training

All USQ employees who provide support services for the USQ ICT environment will be provided with sufficient training and supporting information security awareness tools to enhance awareness and educate them regarding the range of threats, the appropriate safeguards to permit them to properly protect and otherwise manage University ICT resources, and the need for reporting suspected problems.

All new ICT employees will attend induction sessions where they will be introduced to the ICT policy framework and will be provided with access to information and further resources to assist them to become familiar with their roles and responsibilities and understand the security requirements.

Training materials should communicate that information security is an important part of the University's business processes, and will be reviewed regularly.

The level and amount of training in information security threats and safeguards provided to ICT staff must be commensurate with each job holder's individual responsibility for configuring and maintaining information security safeguards. Where ICT staff change jobs, their information security needs must be reassessed and any new training provided as a priority.

3.2 Client Training

Clients must be made aware of the security procedures to observe and the correct use of ICT resources. The *ICT Standard for the Use of ICT Resources* underpins the security awareness program.

Clients and other users of University information resources will be provided with sufficient supporting material to permit them to use the University's ICT resources in a secure manner.

Wherever feasible, clients must be advised of their authorised access privileges and responsibilities when they first obtain access to a specific information resource. (Eg. System logon message).

3.3 Security in Job Descriptions

All USQ staff have some level of access to vital information about University ICT resources. As staff levels increase, so to is the likelihood of increased financial, human resource and other ICT resource delegation. The University defines specific 'delegation' ratings that indicate senior staff positions that hold a particular delegation level.

Where appropriate, staff position descriptions for nominated positions must indicate the general level of access required to University ICT resources. Any general responsibilities for implementing or maintaining security policy, as well as specific responsibilities for the protection of particular assets, or for the execution of particular security activities, must also be included.

3.4 Outsourcing and Third-Party Access

Outsourcing and Third Party Access sets out the conditions that are required to maintain security of USQ's information and systems when third parties, other than our staff and students are involved in their operation. This may arise in three distinct circumstances:

- When third parties are involved in the maintenance, design, development or operation of ICT systems for the University;
- When access to the University's ICT systems is granted from remote locations where computer and network facilities are not under the supervision and control of the University (See also 3.8 Offsite Use of ICT Resources and Mobile Computing); and
- When clients who are not members of the University community are given access to information or ICT systems.

Before engaging third parties and granting them access to ICT systems, resources or facilities, the risks to the University regarding the engagement of the third party shall be identified and appropriate controls implemented prior to granting access.

All identified security requirements shall be addressed before granting clients access to the University's information or assets. Any agreements with third parties involving accessing, processing, communicating or managing the University's information or ICT facilities, or adding products or services to the ICT facilities shall cover all relevant security requirements.

Appropriate security controls, service definitions and delivery levels will be included in any third party service delivery agreement or contract and monitored to ensure they are implemented and complied with by the third party. The services, reports and records provided by the third party will be regularly monitored and reviewed. Changes to the provision of services and support by third parties shall be managed and reviewed on a regular basis taking into account the criticality of University systems and processes involved and any re-assessment of risks.

All third parties who are given access to the University's information systems must agree to follow the information security policies and standards of the University. A summary of the information security policies and standards and the third party's role in ensuring compliance will be provided to any such third party prior to their being granted access.

The University will assess the risk to its information, and where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, the University will require external suppliers of services to sign a confidentiality agreement to protect its information assets.

Any persons responsible for negotiating maintenance and support contracts will ensure that the contracts being signed are in accord with the University's information security policies and standards.

All contracts with third parties for the supply of ICT services to the University must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another vendor.

Any persons responsible for negotiating outsourced development of ICT systems and services must use reputable companies that operate in accordance with recognised standards and will follow the University's information security policies and standards, in particular those relating to application development.

Any facilities management, outsourcing or similar company with which the University may do business must be able to demonstrate compliance with the University's information security

policies and standards and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

3.5 Separation Processes and Movement within the University

Staff accounts will be disabled on their last day of employment. Human Resources will implement a month grace period in the case of casual staff. Departing staff are to be treated sensitively, particularly with regard to the termination of their access privileges. Departing staff must return all ICT assets and equipment belonging to the University, unless agreed otherwise with the designated owner responsible for the information asset.

Exit interviews and associated processes will be implemented to ensure that access to sensitive and secure ICT resources is appropriate. Controls and procedures for terminated or exiting employees should include revoking of access rights and disablement of user logons, collection of keys, access devices, credit cards, etc. Similar processes should also be enabled when students cease to be enrolled in accredited University programs.

It is also critical that processes are implemented to ensure that staff that move to a different role within the University have access provisions that are appropriate to their new role and that access provisions from previous roles are revoked. Where staff change jobs, their information security needs must be reassessed and any new training provided as a priority. Implementation of an exit process will assist to ensure that access provisions are appropriate to the role of specific staff members.

3.6 Confidentiality Agreement

As a condition of gaining access to any University ICT system that contains sensitive or confidential information, employees are required to acknowledge the need to protect the confidentiality of information, both during and after their employment with the University. The requirement for non-disclosure must be communicated at the commencement of their duties.

Non-disclosure agreements must be used in all situations where the confidentiality, sensitivity or value of the information being disclosed is important.

3.7 Reporting Incidents and Violations

You must report any security incidents, security weaknesses, system malfunctions or potential security incidents immediately to any one of the individuals listed in the [ICT Standard for the Use of ICT Resources](#) (Appendix A).

Where appropriate, serious security incidents will result in a Security Incident Report being compiled and referred to the specific Core Process Steward or Principal Activity Steward for attention.

3.8 Offsite Use of ICT Resources and Mobile Computing

To prevent loss, damage, theft or compromise of ICT assets and interruption of the University's activities, security measures shall be applied to off-site equipment taking into account the different risks of working outside the University's premises.

Persons accessing ICT systems and resources remotely to support the University business activities must be authorised to do so by an appropriate Manager or Supervisor within the University. A risk assessment, based on the criticality of the information asset being used, must be carried out.

Each individual Faculty or Organisational unit is responsible for authorising and recording the person/s responsible and location of any University ICT resources used remotely from University premises in their off-site asset register.

Whenever, USQ ICT equipment is to be used remotely from a USQ campus, staff must contact ICT to ensure that all reasonable risks associated with this activity have been considered and ensure that the equipment is subject to compliance with the USQ security standards.

Staff must ensure that all unnecessary information is removed from the equipment prior to its removal from University premises. The information permitted to remain on the equipment should be restricted to that which is required to perform the task identified in the business requirement.

Where the information that remains on the equipment is considered to be sensitive in nature, additional care must be taken to ensure that access to the equipment is restricted to authorised users only.

The employee or student using the equipment must ensure that information is routinely backed up and that the equipment is stored in a safe and secure area at all times.

In the event of damage or loss of an ICT resource, it must be immediately reported to the appropriate Manager or Supervisor in writing, detailing the events that led to the damage or loss of the resource.

The University will publish guidelines in the [ICT Standard for the Use of ICT Resources](#) to advise clients using mobile computing equipment on measures to consider to assist them comply with the University's information security policies and standards

3.9 Disciplinary Process

Penalties and Disciplinary action are outlined in Section 8 of the *USQ Policy for ICT Information Management and Security*.

4 Related Documents

Document (Electronic)	ICT Standard for the Use of ICT Resources available at
	http://www.usq.edu.au/resources/ict_standard_for_the_use_of_ict_resources.pdf