

(Standard) ICT Standard for Operational Security Management

Document Purpose

Document Purpose	<p>This standard defines the Operational security controls implemented by the University.</p> <p>This standard is consistent with, and should be read in conjunction with:</p> <ul style="list-style-type: none"> • ICT Standard for Computer Passwords and System Access Controls • ICT Standard for Information Asset Classification and Control • ICT Standard for Networks • ICT Standard for Physical and Environmental Security. 			
Document Information	Version	1.0		
	Release Date	November 2009		
	Release Status	Final		
	Review Date	November 2010		
	Author(s)	Principal Manager – Infrastructure and Systems		
	Owner	Principal Manager – Infrastructure and Systems		
	Print Date	Last Printed: 21/06/2010 12:27:00 PM		
	Approved By	Principal Manager – Infrastructure and Systems		
	Policy	USQ ICT Policy for Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/resources/ict_standard_for_operational_security_management.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 Operational Procedures and Responsibilities	4
3.1.1 Documented Operating Procedures.....	4
3.1.2 Operator Logs	4
3.1.3 Incident Management Procedures.....	4
3.1.4 Segregation of Duties.....	4
3.1.5 Separation of Development and Operational Facilities.....	5
3.2 Operational Change Control	5
3.3 System Planning and Acceptance	5
3.3.1 Capacity Planning	6
3.3.2 Availability Planning	6
3.4 Protection from Malicious Software	6
3.5 Patch Management	7
3.6 Secure Builds	8
3.7 Backup and Recovery	8
3.7.1 Data Back-up.....	8
3.7.2 Data Recovery.....	8
3.8 Network Management	9
3.9 Data and Software Exchange	9
4 Related Documents.....	10

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 ensure that operational procedures and controls will be documented and implemented ensure that information, information systems and network tasks are managed securely and consistently, in accordance with the level of required security. The University will ensure that:

- Incident management procedures and mechanisms to review violations are in place to ensure appropriate responses in the event of security incidents, breaches or failures;
- Adequate controls are in place for the prevention, detection, removal and reporting of attacks of malicious and mobile code on information systems and networks;
- Comprehensive systems maintenance processes and procedures including operator and audit/fault logs and information backup procedures are in place;
- Operational change control procedures are implemented to ensure that changes to information processing facilities and systems are appropriately approved and managed;
- Methods for exchanging information in all forms, between agencies and/or third parties are compliant with legal and legislative requirements and consistent with the classification schemes and controls defined in the [ICT Standard for Information Asset Classification and Control](#);
- On-line transactions and services are assessed against and are consistent with the requirements of [ICT Standard for Information Asset Classification and Control](#).

All AUSCERT alerts and advisories should be reviewed and prioritised by the ICT Security Officer as soon as possible.

The level of detail and formality of procedures required to manage and operate computer and network services may vary depending on the type of equipment, and nature and sensitivity of the systems application. In principle, the same security management procedures should be applied, with appropriate interpretation of the points mentioned.

Operating systems to be maintained at the latest version release wherever possible. All recommended security patches are to be applied as soon as practical.

3 Standards

3.1 Operational Procedures and Responsibilities

Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter these areas shall be provided with information on the potential security risks and the measures used to control them.

The procedures for the operation and administration of the Universities' business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

Procedures will be established for the reporting of software malfunctions and faults in the Universities' information processing systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

3.1.1 Documented Operating Procedures

The strategies and methods employed in protecting University information resources, the associated responsibilities of users and their ethical and lawful use will be clearly documented as specified in the *USQ Policy for ICT Information Management and Security*, [ICT Standard for the Use of ICT Resources](#) and any supporting standards, procedures and documentation.

3.1.2 Operator Logs

Computer operators and system administrators shall maintain a log of all work which may impact upon the efficient and effective operation of the resource. The logs shall be subject to regular, independent review against defined operating and administration procedures.

3.1.3 Incident Management Procedures

Procedures will be established and widely communicated for the reporting of flaws, incidents and suspected security weaknesses in the Universities' business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents.

Whenever a major security incident indicates that the security of a University information resource is insufficient, prompt remedial action shall be taken to reduce the exposure of all University information resources.

3.1.4 Segregation of Duties

Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University.

Segregation of duties minimises the risk of negligent or deliberate system misuse and consideration shall therefore be given to separating the management or execution of certain duties, or areas of responsibility, in order to reduce the opportunity for unauthorised modification or misuse of data or services.

3.1.5 Separation of Development and Operational Facilities

Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures.

Development and testing activity may unintentionally impact upon the operation of an information resource when conducted on production systems.

Segregation of development and production systems is therefore desirable wherever possible, to reduce the risk of accidental changes or unauthorised access to operational software and master university data.

3.2 Operational Change Control

Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.

The *ICT Procedure for Change Management* outlines the processes adopted by ICT in delivering operational change control of ICT systems and services to the University. The goal of the Change Management process is to ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of changes upon service quality and business continuity, change impact, resource requirements and change approval. This considered approach is essential to maintain a proper balance between the need for change against the impact of the change. It is particularly important that Change Management processes have high visibility and open channels of communication in order to promote smooth transitions when changes take place.

3.3 System Planning and Acceptance

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the University must follow a formalised development process.

The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources.

Acceptance criteria for new information resources shall be defined as part of the existing USQ tender process.

3.3.1 Capacity Planning

Appropriate procedures shall be implemented to monitor the utilisation of key system resources, such as processor, main memory, disk storage, printers and other output devices, and network communications facilities.

The ICT Datacentre Manager shall monitor trends in usage to identify and avoid potential bottlenecks that might present a threat to system security or user services, and to plan appropriate remedial action.

3.3.2 Availability Planning

An emergency fallback facility provides an alternative, temporary means of continuity processing in the event of any damage to or failure of information resources.

ICT managers shall ensure that proper consideration is given to appropriate fallback procedures for all information resources critical to the operation of the University.

Where we have fallback facilities and procedures, these shall be regularly tested.

Such matters should form part of the business continuity plan for the resource.

3.4 Protection from Malicious Software

This standard defines responsibility for protection from computer malware, viruses, spyware, and other malicious code, and the strategy that is to be implemented and maintained at USQ.

The potential for malicious damage on standalone computers is considerable, and is even greater on networked computers due to the speed and ease with which malware can spread across networks.

Computer malware can cause costly damage in terms of reputation, lost information, and productivity. As a consequence, it is imperative the University adopt, and rigorously adhere to, a comprehensive malware control strategy incorporating education, protection, detection, reaction and recovery measures to reduce the likelihood of a malware outbreak and to minimise potential damage.

1. To protect the integrity of software and information
 - a. Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented;
 - b. Where the use of mobile code is authorised, the configuration shall ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code shall be prevented from executing.
2. Any activity with the intention to create and/or distribute malicious software by means of the University of Southern Queensland networks is strictly prohibited.
3. The University of Southern Queensland will employ malware management measures at appropriate ingress and egress points of the University networks. Particular attention will be applied to application gateways.
4. The University of Southern Queensland will implement malware control procedures on all operational computer equipment to ensure that all computer servers and workstations are protected to minimise exposure.
5. To provide cost effective solutions for USQ departments and staff, the Division of ICT Services will negotiate and maintain a site-licence(s) for anti-malware protection application software.

6. The University of Southern Queensland will promote the widespread use of malware control measures to staff and students, and will provide appropriate information and guidelines dealing with their correct use.
7. The University of Southern Queensland will provide all University staff with access to supported malware detection and prevention software applications for use on privately owned computers. Where such computers are to be connected to the USQ network, staff are responsible for ensuring that anti-malware software on these computers is operational and is regularly updated.
8. University of Southern Queensland students residing in residential colleges on-campus will be required to install and maintain current approved malware control as a condition of being permitted to connect a privately owned computer to the University network.
9. Staff will ensure that the malware protection software installed on their workstation is in accordance with this standard, is operating and regularly updated as prescribed, and is not tampered with or removed. Staff will not de-activate or tamper with anti-malware software installed on their computer.
10. Some malware has the ability to damage, disable, or remove installed anti-malware software. If the installed anti-malware software fails to operate normally on a computer server or workstation, then it should be updated and a full scan conducted of the local file system, or reported to the ICT Service Desk.
11. If a computer is known to be infected, it will be removed from the University network until it has been successfully disinfected. ICT staff can assist individuals with recovery from infections, and the steps taken will include containment, disinfecting the system, and capture of relevant incident information.
12. Staff will report all malware infections or reasonable suspicion of infections to the ICT Service Desk. Note that incidents where malware is detected by anti-malware software do not need to be reported. Incidents where malware has successfully infected a USQ computer, or the source of the attempted infection is another USQ computer, should be reported.
13. The Division of ICT Services will report significant malware incidents as part of standing reports to ICT Strategy Committee.

3.5 Patch Management

The *ICT Standard for Patch Management* outlines the patch management strategy adopted by the University. Applying patches or workarounds to mitigate known vulnerabilities can be complex, time consuming and resource intensive, however the application security updates in a timely manner is critical to maintaining the confidentiality, integrity and availability of University information and information systems.

To effectively manage the resources required for patch management and to reduce the threat of security attacks, proactive action will be required to minimise the number of supported versions of operating system, database and application software. Active monitoring will be undertaken to identify vulnerabilities and patches for the supported versions of software.

Available patches will be assessed, tested and prioritised in accordance with resource constraints and the criticality of the applicable information systems.

Where possible patches will be centrally deployed and client-based operating system and application software will be configured for automatic updates.

3.6 Secure Builds

To effectively manage and support the hardware environment, procedures will be developed and documented to ensure that hardware environments, operating systems and core applications are installed in a consistent manner with appropriate versioning and patching levels maintained across all platforms.

3.7 Backup and Recovery

The *ICT Standard for Data Backup* outlines the backup management strategy adopted by the University. Backup and recovery is implemented to ensure continuous business operation, and business can maintain access to data and information within a timely manner should problems occur. Routine backup and recovery is sound data and information management practices and supports the University Business Continuity Policy and Procedures.

3.7.1 Data Back-up

Specific Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsors must ensure that appropriate backup and system recovery procedures are in place and they should specify any special data retention requirements in accordance with the Business and Legislative Policy requirements.

Backup of the organisation's information assets and the ability to recover them is an important priority. The Data Centre Manager is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business.

The Data Centre Manager must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent.

Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

To maintain the integrity and availability of information and information processing facilities, backup copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

Sufficient backups will be retained to recover the system in event of failure in accordance with system BCP requirements. These copies will be kept in a secure location off site. Suitable media management procedure for the identification of particular tapes will be implemented. These should be tested at regular intervals.

3.7.2 Data Recovery

All backup data is accessible through data restoration. Data restores are performed within a physically secure area of DICTS by authorised DICTS employees.

3.8 Network Management

The *ICT Standard for Networks* identifies the network access and operations strategies that have been implemented to ensure the security and integrity of the USQ ICT network. The standard covers areas including the University's internal data communications network, devices connected to it and the Universities connection to AARNet and the Internet.

3.9 Data and Software Exchange

Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorised to receive such information, but the procedures and information security measures adopted by the third party must also be seen to continue to assure the confidentiality and integrity of the information. Refer to the *ICT Standard for Information Asset Classification and Control* for details regarding communication and exchange of specific classifications of information and the requirement for a Confidentiality Agreement to be signed with the third-party organisation.

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
Document (Electronic)	ICT Standard for Computer Passwords and System Access Controls available at http://www.usq.edu.au/resources/ict_standard_for_computer_passwords_and_system_access_controls.pdf
Document (Electronic)	ICT Standard for Information Asset Classification and Control available at http://www.usq.edu.au/resources/ict_standard_for_information_asset_classification_and_control.pdf
Document (Electronic)	ICT Standard for Networks available at http://www.usq.edu.au/resources/ict_standard_for_networks.pdf
Document (Electronic)	ICT Standard for Patch Management available at http://www.usq.edu.au/resources/ict_standard_for_patch_management.pdf
Document (Electronic)	ICT Standard for Physical and Environmental Security available at http://www.usq.edu.au/resources/ict_standard_for_physical_environment_security.pdf