

(Standard) ICT Standard for System Development and Maintenance

Document Purpose

Document Purpose	<p>This standard defines what controls will be implemented by the University in relation to System Development and Maintenance.</p> <p>This standard is consistent with, and should be read in conjunction with:</p> <ul style="list-style-type: none"> • ICT Standard for Operational Security Management. 			
Document Information	Version	1.0		
	Release Date	July 2008		
	Release Status	Final		
	Review Date	July 2009		
	Author(s)	Principal Manager – Infrastructure and Systems		
	Owner	Principal Manager – Infrastructure and Systems		
	Print Date	Last Printed: 7/09/2009 2:22:00 PM		
	Approved By	Principal Manager – Infrastructure and Systems		
	Policy	USQ Policy for ICT Information and Security Management		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/ict/~media/USQ/ICT/ICTStandardforSystemDevelopmentandMaintenancepdf.ashx		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2008	Various	Document creation
	1.0	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 Error! Bookmark not defined.**
- 3 Standards..... 5**
 - 3.1 Security Requirements of Systems..... 5
 - 3.2 Systems Design and Development Requirements 5
 - 3.3 Systems Testing and Implementation..... 6
- 4 Related Documents..... 7**

1 Definitions

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

2 Broad Guidelines

When establishing new systems or implementing improvements to current information systems including off-the-shelf or outsourced software development, the University will ensure that appropriate practices and principles are adhered to including:

Security:

- The University will ensure that security controls are in place during all stages of system development, including when new systems are implemented into the operational environment. Such controls must be commensurate with the security classification of the information contained within, or passing across, information systems, networks infrastructures and applications
- Security requirements are addressed in the specifications, analysis and/or design phases and that internal and/or external audit are consulted when implementing new or significant changes to financial and critical business information systems;
- Processes including data validity checks, audit trails and activity logging are included in applications to ensure the accuracy and integrity of data captured or held in applications; Authentication techniques and policies are consistent with those requirements defined in the *ICT Standard for Information Asset Classification and Control*;
- That access to system files is controlled to ensure integrity of the business systems, applications and data; and
- Access controls including access restrictions and segregation/isolation of systems are identified and implemented into all infrastructures, business and user developed applications.

Hosting and Deployment:

- Specific hosting and deployment strategies will be selected as to maximise redundancy and uptime within available resources.
- Where necessary environments other than production should be maintained in as close to production specifications and configurations as possible. This allows for timely and accurate testing and troubleshooting.
- Where development is being undertaken in house a three tier approach of development, testing and production should be used.
- Where external hosting is used, contractual issues with regard to ownership and use of data before, during and after hosting, needs to be scrutinized.

Change Management:

- Appropriate change control, acceptance and system testing, planning and migration control measures are carried out when upgrading or installing software in the operational environment;

Technology Support:

- New products and technologies should be investigated with regards to the current set of supported technologies particularly considering skill sets and additional costs.

- The converse of the above is the continual use of older technologies when they have ceased to be supported or commonly used in the industry. Work done on archaic platforms will likely need to be done again if the platforms and technologies are replaced.

Standards of Coding Development and Documentation:

- Where code development, documentation and systems development procedures and methods have been developed, they should be used throughout the teams in that section. Disparate methods lead to complexity and bad communications.
- Before new development takes place with new technologies procedures for code development and documentation should be developed.

3 Standards

The development, procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by the organisation must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. The USQ Project Management Methodology provides the respective Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor for each core ICT system with a number of templates and examples that are recommended during the phases of startup, initiation, implementation, completion and review. Use of this methodology is recommended but will be dependent on the size and scope of any proposed systems development or maintenance activities.

The respective Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor for each core ICT system with the assistance of the Project Board and Project Manager will ensure that the business requirements and information security requirements are addressed in the specifications, analysis and design phases of any new ICT project or enhancement to an existing system.

3.1 Security Requirements of Systems

All relevant information security requirements and controls, including business continuity and disaster recovery, shall be identified during the requirements phase of any ICT project or upgrade, and agreed to prior to the development or procurement of information and communication technology systems and resources. Any potential risks, vulnerabilities or conflicts with existing systems or business processes shall be identified and addressed.

Access controls - including access restrictions and segregation/isolation of systems - shall be identified and implemented into all systems and resources.

Any patch management issues shall be considered and addressed prior to the implementation of systems and resources.

3.2 Systems Design and Development Requirements

The respective Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor or their delegated representative, typically the Project Manager, will ensure that the design and development activities associated with a new ICT project or enhancement to an existing system is consistent with the system specification and requirements.

The Project Manager shall be responsible for the security of the associated development, testing and support environment. The Project Manager shall ensure that all proposed modifications are reviewed to ensure that they do not compromise the security of either the production system, or the development and support environment.

Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. 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. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.

Modifications to vendor supplied software shall be discouraged, only strictly controlled essential changes shall be permitted and the development of interfacing software shall only be undertaken in a planned and controlled manner.

The implementation, use or modification of all software on the organisation's business systems shall be controlled. Quality control procedures will be in place to assure the quality of released code and to protect against malicious code. For systems where code is not available a risk assessment must be made with regards to malicious intent.

3.3 Systems Testing and Implementation

Input data shall be validated to ensure that it is both correct and appropriate for the system application.

Test data shall be selected carefully, and protected and controlled.

Data which has been correctly entered into an information system can be corrupted by processing errors or through deliberate acts. Validation and integrity checks shall be built into systems to detect such corruption.

4 Related Documents

Document (Electronic)	ICT Procedure for Change Management http://usqindex.usq.edu.au/sits/ictindex/Procedures_&_Processes
Document (Electronic)	ICT Standard for Information Asset Classification and Control http://www.usq.edu.au/ict/~media/USQ/ICT/ICTStandardforInformationAssetClassificationandControlpdf.ashx
Document (Electronic)	ICT Standard for Operational Security Management http://www.usq.edu.au/ict/~media/USQ/ICT/ICTStandardforOperationalSecurityManagementpdf.ashx