

(Standard) ICT Standard for Computer Passwords and System Access Controls

Document Purpose

Document Purpose	<p>This standard defines the control mechanisms based on business owner requirements and assessed/accepted risks that must be in place for controlling access to all information, information systems, networks (including remote access), infrastructures, and applications.</p> <p>Where a computer system is not nominated, this standard should be recognised as specifying the minimum requirements.</p> <p>This standard is consistent with, and should be read in conjunction with:</p> <ul style="list-style-type: none"> • ICT Standard for Information Asset Classification and Control • ICT Standard for Networks • ICT Standard for the Use of ICT Resources 			
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 12:22:00 PM		
	Approved By	Principal Manager – Infrastructure and Systems		
	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_computer_passwords_and_system_access_controls.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 Business Requirement for System Access.....	4
3.1.1 Documented Access Control Policy	4
3.2 User Access Management	4
3.2.1 Privilege Management.....	5
3.2.2 User Password Management	6
3.2.3 Review of User Access Rights	6
3.3 System Planning.....	7
3.4 Network Access Control	7
3.5 Application Access Control.....	8
3.5.1 Information Access Restrictions	8
3.5.2 Use of System Utilities	8
3.5.3 Access Control to Program Source Library	8
3.5.4 Classified System Isolation	8
4 Related Documents.....	9

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 Queensland Government Authentication Framework provides the University with guidance with regard to determining the authentication requirements for services. ICT in collaboration with specific Corporate Executive Portfolio Stewards/Principal Activity Stewards/System Sponsors will implement access control policies and procedures that address and detail access control rules and rights for each group of clients. Generally these will be based on “what must be generally forbidden unless expressly permitted” ensuring that business requirements are followed. The overall framework for access rights should be reviewed regularly to ensure that they remain appropriate.

The standard will identify and define specific policy and procedures for the:

- Access to University information systems including specific authorisation and that each user is assigned an individually unique personal identification code and secure means of authentication;
- Management of operating systems security, including user registration, authentication management, access rights and privileges to systems or application utilities;
- Restricted access and authorised use only warnings are displayed upon access to all University systems;
- Where wireless communications are used, that the security features of the product are appropriately configured and afford at least the equivalent level of security of wired communications;
- Control measures are implemented to detect and regularly log, monitor and review information systems and network access and use, including all significant security relevant events;
- Risk assessments are conducted and policies and processes are defined for mobile technologies and teleworking facilities; and
- Security risks associated with use of ICT facilities and devices (including non-University equipment) within the University such as mobile telephony, personal storage devices and internet and email, are assessed prior to connection and appropriate controls implemented.

3 Standards

3.1 Business Requirement for System Access

Access to computer services and corporate data will be controlled on the basis of business requirements. Access to University information resources will only be provided on a need-to-know basis at the discretion of the relevant Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor.

Access to such information will normally be denied until authorised by the appropriate authority.

3.1.1 Documented Access Control Policy

Business requirements for access control to core information systems and information resources should be defined and documented during the development of the relevant Information System Plan/Procedures and approved by the relevant Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor.

Each Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor should maintain a clearly defined access policy statement for Information Systems that they are responsible for, which defines the access rights of each clients or group of clients.

Consideration should be given to the establishment of standard client access profiles for common classifications of users of University information resources.

3.2 User Access Management

The Identity Management System (IDM) is the access control system used to automate the creation of user accounts to access USQ computer systems and ICT resources. As new systems are introduced and existing systems updated, the intention is to progressively migrate all ICT resource access registration processes through IDM. Provisioning of resource access to a user account is allocated on the basis of a user's classification (eg. staff, student, third party).

The primary means of security of the University's information resources is through the allocation of individual computer accounts and access passwords. It is every user's responsibility to ensure that:

- Passwords are selected carefully and not shared with other persons,
- Computer workstations are kept physically secure, and
- Computer accounts are not shared with other persons.

Group accounts will require authorisation from the appropriate Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor.

Access to all information services shall use a secure log on process in accordance with the information classification system. All access to core system information services is to be logged and monitored to identify potential misuse of systems or information.

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all client access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff. Where possible the procedures shall be managed to ensure consistency across the

University, and to assist with the automatic creation, temporary closure and deregistration of accounts.

Access to multi-user systems should be controlled through a formal user registration process which should consider the following:

- Access to all systems must be authorised by the Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted.
- Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the organisation. Users' access rights will be reviewed at regular intervals.
- Provides users with an explanation of their access rights and privileges.
- Requires clients to indicate their acceptance of the conditions of access and the associated obligations and responsibilities.
- Maintenance of a formal record of all clients registered to use a service
- Remove the access rights of a client as soon as practicable whenever their requirements are altered. For example, when the change positions, classification or leave the employ of the University.
- Periodic checks should be made for, and remove, redundant accounts that are no longer required
- Accounts which are not used for an extended period of time may be locked from further access until the users access status can be verified with the client.
- Ensure that redundant or duplicate user identifiers are not issued to another client.

3.2.1 Privilege Management

The use of special system privileges shall be restricted and controlled based upon the least privilege principle. The allocation of privileges shall be controlled through a formal authorisation process which takes into consideration the following where relevant:

- Maintain an authorisation procedure and a record of all privileges allocated.
- Maintain a log of all access to system privileged accounts, for example the UNIX superuser account
- Access to the UNIX superuser account should only be permissible from either the system console, or from an individual system administrator's personal account. Such increases in user privileges should be securely logged for audit purposes and only used when absolutely required. Users with access to the system privileged accounts should be assigned a different user identifier for normal system use.
- Promote the development and use of operational procedures which avoid the need to grant privileges in excess of the requirements for the current task.

3.2.2 User Password Management

Wherever possible, consistent password rules will apply across all ICT systems. Allocation of all passwords (ie. user, administration and application) shall be controlled by a formal management procedure. Requirements will vary according to the information resource operating system, but in all cases the following issues will be considered:

- All computer accounts which provide access to a University information resource must be protected by a suitable password management system
- It is every client's responsibility to ensure that passwords are selected carefully and not shared with other persons
- Users should initially be provided with a secure password which they are forced to change when first accessing the account, where this is permitted by the ICT system.
- An appropriate password ageing procedure is implemented.
- Passwords must be conveyed to the client in a secure manner. The use of unprotected electronic mail (clear text) is not considered a secure method of either requesting or informing a client of an account password. Individual passwords should not be printed, stored online, transmitted via electronic mail, or given to others. Having said this, email may be used in rare instances to expedite business processes.
- All requests for passwords must be subject to appropriate identification of the client. Conveyance of account passwords through third parties shall be avoided.
- No clear text record of passwords assigned to any account shall be maintained unless done so in a secure manner in isolation to the associated information resource.
- Additional security procedures will be required for the management of passwords for system privileged accounts which may need to be shared amongst more than one authorised administrator.

The University of Southern Queensland will promote the widespread use of passwords to staff and will provide appropriate information and guidelines dealing with their correct use. Individuals are responsible for all transactions where access via a password mechanism applies. As a consequence, no individual shall access any computer system with any other individual's password.

3.2.3 Review of User Access Rights

Whenever a client ceases to need, either wholly or in part, the access privilege they currently possess, appropriate notification should be relayed by the clients manager or supervisor to ICT indicating the change in status. Where possible, such notification should occur before the change in status.

In addition, consideration shall be given to the adoption of a formal procedure to review all access privileges to information resources on a regular basis. Special attention should be made to the system privileged accounts.

3.3 System Planning

New information systems, or enhancements to existing systems, must be authorised jointly by the Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor responsible for the system and the CTO. The business requirements of all authorised systems must specify requirements for security controls.

The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

The information assets associated with any proposed new or updated systems must be identified, classified and recorded, in accordance with the [ICT Standard for Information Asset Classification and Control](#), and a risk assessment undertaken to identify the probability and impact of security failure.

Equipment supporting business systems shall be planned to ensure that adequate processing power, storage and network capacity are available for current and projected needs, all with appropriate levels of resilience and fault tolerance. Equipment shall be correctly maintained.

Equipment supporting business systems shall be given adequate protection from unauthorised access, environmental hazards and failures of electrical power or other utilities.

Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the University's information security policies, standards and requirements for ongoing information security management.

3.4 Network Access Control

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.

3.5 Application Access Control

Logical access controls should be enforced to control authorised access to application systems and data held within information resources. Systems should:

- Control client access to data and application systems functions, in accordance with the *USQ Policy for ICT Information Management and Security*;
- Provide protection from unauthorised access for any utility software that is capable of overriding system or application controls; and
- Not compromise the security of other systems with which information resources are shared.

3.5.1 Information Access Restrictions

Enforcement of the following controls should be considered in order to support access policy requirements:

- Use of menus to control access to application system function;
- Only provide access to system documentation on a need to know basis;
- Enforcing the minimum access capabilities (read, write, execute, create and delete) needed by users to meet their requirements;
- Ensure that output from application systems which handle sensitive data contain only the data that are relevant to the use of the output.

3.5.2 Use of System Utilities

It is essential that use of application utilities that have additional system privileges is restricted and tightly controlled. Consideration should be given to the enforcement of the following controls:

- Secure access to system utilities;
- Segregation of system utilities from applications software;
- Limit the privilege of the system utility to the minimum level required to successfully meet its intended purpose;
- Limitation of the use of privileged system utilities to the minimum number of authorised users;
- Removal of all unnecessary utility and system software.

3.5.3 Access Control to Program Source Library

To minimise the possible corruption of computer programs, strict control may be required over access to program source libraries. The *ICT Procedure for Change Management (restricted access)* outlines the processes adopted by ICT in delivering operational change control of ICT systems and services to the University.

3.5.4 Classified System Isolation

Information resources that are classified as secure or sensitive may require a specific computing environment as defined in *the ICT Standard for Information Asset Classification and Control*.

4 Related Documents

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 the Use of ICT Resources available at http://www.usq.edu.au/resources/ict_standard_for_the_use_of_ict_resources.pdf