

Replaces (please remove) Section 10.8, Issue 02/06

## 10.8 POLICY FOR COMPUTER PASSWORDS

### 1 Preamble

The University Information and Communication Technology Resource Security Guidelines <http://www.usq.edu.au/resources/1051.pdf> recognise the importance of password management and the adoption of an appropriate password management system. The primary means of security for the University's information and communication technology resources is through the allocation of individual computer accounts and access passwords. It is every client's responsibility to ensure that passwords are selected carefully, changed regularly and not shared with other persons.

### 2 Purpose

This policy defines the computer password measures for nominated computer systems that are to be implemented and maintained at USQ. Where a computer system is not nominated, this policy should be recognised as specifying the minimum requirements. It is consistent with and should be read in conjunction with the USQ Policy for Information and Communication Technology Security Management <http://www.usq.edu.au/resources/1051.pdf>, USQ Policy of the Use of Information and Communication Technology Resources <http://www.usq.edu.au/resources/101.pdf> and the Code of Practice for the Acceptable Use of Information and Communication Technology Resources <http://www.usq.edu.au/resources/103.pdf>.

Passwords provide a measure of security and protection to an individual's computer resources and services. They also protect an individual's privacy and reputation where files and electronic mail cannot be accessed by others or misused by others to slander, defame, embarrass or implicate another individual in illegal or unethical activities. Therefore, it is imperative that appropriate measures are implemented to ensure that individuals are educated as to the proper management, use and selection of appropriate passwords and that passwords are changed regularly.

This policy applies to all users of ICT resources and ICT equipment owned, leased or rented by University of Southern Queensland. This includes, but is not limited to:

- academic staff,
- visiting academic staff,
- administrative staff,
- guests of University staff and
- external individuals or organisations.

### 3 Policy

3.1 The University of Southern Queensland will ensure that access to University Information and Communication Technology administrative resources is controlled through the allocation of individual computer accounts and access passwords. It is every client's responsibility to ensure that passwords are selected carefully and not shared with other persons.

3.2 The University of Southern Queensland Password requirements will vary according to the Information and Communication Technology resources accessed but the following requirements will be addressed:

- Users will initially be provided with a secure password which they are forced to change when first accessing the account.
- An appropriate password aging 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.

- All requests for passwords must be subject to appropriate identification of the client. Telephone requests will be discouraged.
- Conveyance of account passwords through third parties will be avoided where possible.
- No clear text record of passwords assigned to any account will 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.

3.3 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.

3.4 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.

3.5 Passwords do not imply privacy. Use of passwords to gain access to any part of the USQ computer infrastructure or for encoding of particular files or information does not imply that individuals have an expectation of privacy in the material they create or receive on University computer systems. Access to each computer system or service is managed by an Information Resource Manager who has authority to determine all issues related to policy and procedures for each computer system or service.

#### **4 Regulations**

4.1 Password access to the University of Southern Queensland administrative NT servers and systems will be subject to the following minimum guidelines:

- Password must be changed at least every 90 days;
- The minimum password length will be set at six characters;
- A password history file containing the last 10 passwords will be kept to discourage reusing previously used passwords;
- Account lockout will occur after five unsuccessful logon attempts.

4.2 Restoration of passwords that have expired, been forgotten, or lost through unsuccessful access will be reported by the client to system administrators responsible for password access to the particular system under which the situation exists for attention.

4.3 Any breach or violation of this policy will be dealt with under the appropriate USQ staff or student Breach of Discipline regulations.

#### **5 Officer Responsible for Policy Formulation**

Chief Technology Officer, Division of ICT Services

#### **6 Reviewing Body**

ICT Strategy Committee, University of Southern Queensland.

#### **7 Approving Authority**

Vice Chancellor, University of Southern Queensland.

\_\_\_\_\_ Date: \_\_\_\_\_