USER CODE AND PASSWORD POLICY

Section	Information Technology Services
Contact	Information Technology Services
Last Review	June 2013
Next Review	August 2016
Approval	SLT 13/08/174

Purpose:

This Policy is intended to protect Massey University's network infrastructure and information systems from uncontrolled or unauthorised access which may result in intellectual property loss or data destruction.

Policy:

User Codes:

The following applies:

- All University network users (hereafter called "users") will be provided with an individual and confidential Network Usercode (which may be referred to variously as user ID, user code, client code, user name) for their sole use
- Usercodes will be centrally managed.
- The user is responsible for all activity associated with their usercode

Definitions:

Passwords:

The following applies:

- The user will not share their usercode and password details with others.
- The user will not attempt to discover or change any other person's password
- The user will not use their Massey usercode and password to access non-Massey systems.
- Passwords will be robust (at least 7 characters in length and containing at least 2 numbers, punctuation or special characters)
- The system will show staff the strength of the password that they have chosen
- Passwords will be changed from the initial default at the first point of use, and at least every six months thereafter.
- The system will be enabled to remind and support staff to change their password after 90 days
- Passwords will not:
    - contain the words "Massey", "password" or any derivation.
    - contain birthdays, phone numbers or other personal information.
    - use word or number patterns such as aaaabbbb, qwertyui, zyxwvuts, 12344321, etc.

User code and Password management is an individual responsibility and a failure to abide by this policy may result in disciplinary action.

Audience:

All users of Information and Communication Technologies at Massey University including staff, students, contractors and affiliates.

Relevant legislation:

Privacy Act 1993
Copyright Act 1994

Legal compliance:

The Privacy Act 1993 places an obligation on organisations to protect information from inappropriate access by unauthorised parties. Uncontrolled access to the University's network has the potential to make it very easy to gain unauthorised access to University network based resources. However, the Privacy Act 1993 places an onus on organisations to protect information from inappropriate access by unauthorised parties.

There is a significant amount of information held on the University's network that is protected by copyright and it is therefore important to ensure that only appropriate people have access to this resource so that copyright protection is not breached. There is a significant amount of information held on the University's networked systems that is protected by copyright and it is therefore important to ensure that only appropriate people have access to this information, to ensure that copyright protection is not breached.

Related procedures / documents:

Data Network Policy
Internet Use and Digital Communications Policy
Telecommunications Policy
Use and Access to Information Technology Systems Policy
Policy on Staff Conduct
Code of Student Conduct
Contract Management Policy and Contractors (Academic and General Stuff Duties) Procedures

Document management control:

Prepared by: Information Technology Services
Authorised by: Chief Information Officer
Approved by: SLT 13/08/174
Date issued: February 2008
Last review: June 2013
Next review: August 2016