PASSWORD POLICY

Section	Information Technology Services
Contact	Chief Information Officer
Last Review	February 2023
Next Review	February 2026
Approval	SLT 21/02/08

Purpose:

Passwords are the primary form of user authentication used to grant access to Massey's information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to Massey's information systems, and thereby compromising the security of those systems.

Key success factors:

- Massey University's network infrastructure and information systems are protected from uncontrolled or unauthorised access which may result in intellectual property loss or data destruction.
- The availability of University systems and information is restricted to authorised persons only.

Policy:

The Password Policy applies to all information systems, information components, and all users working on behalf of the University. Users include staff and students (including, but not limited to contractors, consultants and volunteers).

The University will use passwords or passphrases (a sequence of words) to protect user accounts, in order to maintain the security of information. To ensure passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that they will be easy to break, thus allowing easier illicit access to Massey's information systems, and thereby compromising the security of those systems. Where this policy refers to passwords it equally applies to passphrases.

Policy Statements:

1. Passwords are to be individually owned and kept confidential. The user will not share their password details under any circumstances.

2. The user will not attempt to discover or change any other person's password.

3. Passwords must be constructed according to a minimum set length (longer is better) and complexity requirements. As such, passwords must:

    - be at least 10 characters in length
    - contain at least 2 numbers, punctuation or special characters.

4. The system will show staff the strength of the password that they have chosen.

5. Passwords will be changed from the initial default at the first point of use, and at least every 90 days thereafter.

6. The system will be enabled to remind and support staff to change their password after 90 days.

7. Passwords will not be easy to guess. They 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.

8. The use of multi-factor authentication for systems that represent a higher risk is required. This is especially valuable for internet-facing systems where the University cannot control the device being used to access the system.

9. Password management is an individual responsibility. Violations of this policy may result in consequences which may include but are not limited to, one or more of the following:

    - disciplinary action
    - termination of employment; and/or
    - legal action according to applicable laws and contractual agreements.

Definitions:

Multi-factor authentication is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication system.

Password is a secret string of characters (letters, numbers, etc) that is used to prove identity.

Passphrase is a secret phrase (made up of words that are easy to remember) that is used to prove identify. For example, il1ke2eatbreakfast.

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:

Acceptable Use of Technology Policy
Code of Student Conduct
Device Security Policy
Information and Technology Security Policy
Staff Conduct Policy

Document management control:

Prepared by: Chief Information Officer
Authorised by: Deputy Vice-Chancellor, University Services
Date issued: February 2008
Last review: February 2023
Next review: February 2026