PASSWORD POLICY

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.

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

u

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: Dep0.00 n9.96 Tf1 0 0 1 36 581.14 Tm0 g0 [(A)4(uth)-7(oris)-2(ed)-7(by5v0 rle)-14(ec)-3(hn)4(o)-9(l)5(og)-7(y)-