Password Standard

> **Compromised passwords?**
>
> If you suspect that your password has been compromised, please change it immediately and alert the Pawsey Help Desk.

The security of your password can influence the security of your Pawsey digital identity as well as the security of resources and services that can be accessed using this identity.

Password security is facilitated using a set of rules.

Password rules

- Minimum 13 characters long
- Is not in the dictionary of known weak passwords
- Different from the last 8 passwords used
- Must be changed every 12 months
- Cannot be changed more than once in 24 hours

The above rules aim for the balance of usability and security.

Having to change passwords once a year minimises user inconvenience whilst providing an acceptable level of protection against common threats that target passwords.

Please refer to additional information below on how to pick a strong password and manage your passwords securely.

Choosing Strong Passwords

We encourage the use of lengthy (20 characters or more) randomly generated passwords that consist of at least 3 character classes (lowercase letters, uppercase letters, digits and special characters).

A password management solution can be used to generate and store random complex passwords in a convenient manner.

As an alternative, you can pick a memorable passphrase, however please be aware that passphrases are not necessarily more secure by default and still need to include a level of randomisation.

Managing Passwords Securely

Password managers can be used to securely handle all your passwords in a single place.

Using a password manager provides various benefits, such as:

- Automated handling of password entry and storage for web-based forms
- Creation of stronger passwords using an integrated generator
- Centralised storage of passwords protected by strong encryption

The main caveat is that usually password managers require a master password that becomes the weakest link.

Therefore, it is crucial to pick a strong master password and explore additional protection mechanisms, such as two-factor authentication (2FA) that may be offered by some solutions.

There are a number of password managers (both free and commercial), some examples:

KeePass (Windows), MacPass (OS X), PasswordWallet (Windows, OS X, mobile), and Password Safe (Windows).

Public Key Authentication

You are encouraged to use public key authentication for Secure Shell (SSH) sessions (e.g. interacting with the supercomputer login nodes).

Both Putty (PuTTYgen) and OpenSSH (ssh-keygen) have facilities for generating keys (please consult the relevant manual pages for specific guidance).

A 2048 bit RSA key is considered appropriate.

Please pick a strong key passphrase when generating a key and store it separately from the key itself. Do not share the private key with anyone.