

## CP.67 ICT Password Management

<i>Responsible Department</i>	Corporate Services
<i>Resolution Number</i>	C.5153
<i>Resolution Date</i>	16/10/2024
<i>Next Scheduled Review</i>	2026/27
<i>Related Shire Documents</i>	Council Policy CP.65 ICT Security Access Council Policy CP.66 ICT BYOD Management
<i>Related Legislation</i>	OAG Information Systems Audit Local Government 2021/22

### OBJECTIVE

This policy aims to preserve the safety and security of electronically stored information and ICT equipment.

A password is required for all accounts and all mobile devices, including Bring Your Own Devices (BYOD) mobile phones.

### SCOPE

This policy is applicable to ICT password management and affects Council Members and employees.

### POLICY

- Passwords are a critical element in maintaining adequate information security and determining the identity of a device user.
- Users must never share their passwords.
- Users must not attempt to use another person's credentials. This includes allowing another person to use their credentials, e.g. logging into the system and allowing another user to use this computer.

#### 1. Password Standards

The following password standards are to be applied to reduce the risk of unauthorised access.

Password Length	Minimum 8 characters in Length
Structure – mix of characters	Must contain at least <b>one Upper Case</b> Must contain at least <b>one special character</b> or <b>numeric value</b> . Must not contain the person's given name, last name or employee ID. Must not be same as the username.
Password expiry	Password expires every 60 days.

Account locked	Account will be locked after 7 invalid password attempts.
How to “unlock” account	<ul style="list-style-type: none"> <li>• Users can wait 15 mins and try again; or</li> <li>• Contact the ICT department in person, by email or by telephone.</li> </ul>
2 Factor Authentication	Staff and Council Members are required to set up 2FA.

## 2. Locking of workstations

Users must lock workstations whenever they are left unattended to prevent misuse of their credentials.