Authority Local Government Act 1995 (WA)(CI)
Local Government Audit Regulations 1996 (WA)(CI)
Regulation 17(a)(b)

ICT1– Information and Communication Technology Systems Security

Objective

This policy provides guidelines for the protection and use of information technology assets and resources within the Shire to ensure integrity, confidentiality and availability of data and assets.

This policy applies to all staff, elected members, contractors and others that are granted system access.

Policy

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through a secure locked door with approved access.

It is the responsibility of Manager Finance & Administration that this requirement is followed at all times.

All security and safety of all portable technology such as laptops, notepads, iPad, mobile phones, etc will be the responsibility of the employees who has been issued with the asset. The employee is required to use locks or passwords and to ensure the asset is kept safely at all times.

In the event of loss or damage, the Manager Finance & Administration will assess the security measures undertaken to determine if the employee will be required to reimburse the Shire for loss or damage.

Information Security

All significant records of the Shire that has an administrative, fiscal, legal value and includes records that relate to Shire business is to be backed up.

It is the responsibility of the Manager Finance & Administration to ensure that data back-ups are conducted daily for server back up and weekly tape backups and the backed up data is as follows:

Daily server Backups

- Backups are done on LTO8 tapes and Veem backup software
- Data on tapes are encrypted
- The most recent tape is taken off site- by Manager Finance & Administration
- Backup tapes that are onsite are kept in secure safe

Network Intrusion

- Antivirus update monthly
- Antivirus logs checked daily
- Antivirus updates pushed out to computers when applicable
- WIFI network logs checked daily
- Firewall logs checked daily
- All servers and UPS have login notification when login in to backend
- Active directory logs checked weekly

Technology Access

IT Officer is responsible for the issuing of initial password for all employees; this will be a temporary password which will be required to be change at first login.
Where an employee forgets the password or is locked out after three attempts, than contact the IT Officer to initiate new password.

Password Set up
Maximum password duration – 90 days (System will force password change after 90 days)
Password must meet the following conditions, these cannot be changed

- Be at least seven characters in length
- Contain characters from three of the following four categories
  1 English uppercase characters (A to Z)
  2 English lower case
  3 Base digits (0-10)
  Non alphabetic characters (for example !,$,#,%)

Staff are not to allow the use of their password to other staff members or external parties to ensure privacy of data is maintained.

Remote access to Shire corporate systems is to be approved by the CEO

Key Performance Indicators	
Keywords	
Related Policies	Nil
Related Procedures/ Documents	
Delegation Level	CEO
First endorsed by Council	
Resolution No.	
Consultation	Nil required
Reviewed by Council	Adopted on 26 April 2022
Resolution No.	36/22
Date Document Updated	/
Next Review Date	April 2024
File Reference	2.11.5