POLICY

PASSWORDS

APPROVALS

POLICY NUMBER	CORP-POL-039	**DOC.ID**	4934205
CATEGORY	Administrative		
POLICY OWNER	Chief Information Officer		
APPROVAL DATE	24/05/2022	**RESOLUTION NUMBER**	7845

ISAAC.QLD.GOV.AU
P 1300 472 227 F 07 4941 8666 A PO Box 97 Moranbah QLD 4744

isaacregionalcouncil isaacregionalcouncil Isaacrcouncil
ISAAC REGIONAL COUNCIL ABN 39 274 142 600

POLICY

OBJECTIVE

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

SCOPE

The scope of this policy includes all personnel who have or are responsible for any form of system access that requires a password and is applicable to all systems employed by IRC.

DEFINITIONS

TERM / ACRONYM	MEANING
IRC	Isaac Regional Council.

POLICY STATEMENT

This policy is an essential part of an overall strategy to protect the security of the Isaac Regional Council (IRC) network, data integrity, and computer systems. All users, including contractors and vendors, with either internal network or remote access to IRC systems are responsible for complying with this policy. All users of IRC computer systems are required to comply with all relevant legislation, regulations and policies applicable to IRC.

GENERAL

Users of Council's systems must take appropriate actions to ensure the security of information held within those systems. As a general guide passwords are changed:

- At least every 90 days for system level passwords (root, administrator, application administration accounts)
- At least every 90 days for user level passwords (network logon, email, web, desktop computer)
- At any time a user suspects their password has been compromised.
- Whenever a user is required to do so by the ICT team.
- Whenever ICT resources automatically prompt the user to do so.
- If an ICT team member is required to reset a user's password for approved access in the user's absence.

The following practices are also required to contribute to the integrity and security of Council systems:

- Passwords must not be inserted into email messages or other forms of electronic communication.
- Users must not write down and store passwords i.e. in diaries, notebooks or files.
- All user level and system level passwords must conform to the strong password guidelines given below.

ISAAC.QLD.GOV.AU
P 1300 472 227 F 07 4941 8666 A PO Box 97 Moranbah QLD 4744
isaacregionalcouncil isaacregionalcouncil Isaacrcouncil
ISAAC REGIONAL COUNCIL ABN 39 274 142 600

REQUIREMENTS

General Password Construction Guidelines

All users at IRC should utilise strong passwords that contain the following characteristics:

- Password must contain at least three of the five character classes listed below:
  - Lower case characters (a b c…)
  - Upper case characters (A B C…)
  - Numbers (1 2 3…)
  - Punctuation (: ; …)
  - Special characters (@ # %...)
- At least ten alphanumeric characters long
- Not words from any language, slang, dialect, jargon
- Not based on personal information, names of family

PASSWORD PROTECTION STANDARDS

Passwords are the frontline protection for user accounts and are an essential element of Council's network security. All employees are responsible for the protection and integrity of their own password/s or any other system password/s by following the standards below:

- Users must not use the same password for IRC accounts as for non-IRC access (e.g., personal ISP account, Internet Banking, EBay etc.).
- Passwords may not be shared with anyone. Employees who wish to delegate access to their email accounts should seek manager approval before doing so through the permissions in MS Outlook. All passwords are to be treated as sensitive, confidential IRC information.
- Never:
- Reveal a password in an email message
- Talk about a password in front of others
- Hint at the format of a password ("my family name")
- Reveal a password on questionnaires or security forms
- Share a password with family members
- Reveal a password to co-workers while on holiday

If a user suspects that an account or password has been compromised, the incident must immediately be reported their manager and ICT and the password change.

ISAAC.QLD.GOV.AU
P 1300 472 227 F 07 4941 8666 A PO Box 97 Moranbah QLD 4744
isaacregionalcouncil isaacregionalcouncil Isaacrcouncil
ISAAC REGIONAL COUNCIL ABN 39 274 142 600

APPLICATION DEVELOPMENT AND CONFIGURATION STANDARDS

Developers/administrators must ensure that functional changes comply with the following security precautions:

- Enforces authentication of individual users, not user groups.
- Does not store passwords in clear text or in any easily reversible form.
- Provides for role management such that one user can access the same functionality as another without having to know the other's password.

AUTHORITIES AND ACCOUNTABILITY

All employees have a responsibility to report security incidents and breaches of this policy so that appropriate action can be taken to remedy breaches. Any act or lack of action by and IRC staff member that contravenes this policy may be subject to disciplinary action.

LEGISLATIONS AND RELATED GUIDELINES

- *Privacy Act 1988*
- *Telecommunications Act 1997*
- *Telecommunications Regulation 2021*
- *Criminal Code Act 1995*

REFERENCES

ID	NAME
CORP-POL-006	ICT Policy – Access to IRC Data
CORP-POL-007	ICT Policy – Network Security
CORP-POL-004	ICT Policy – Use of Electronic Communications
CORP-POL-079	Code of Conduct

ISAAC.QLD.GOV.AU
P 1300 472 227 F 07 4941 8666 A PO Box 97 Moranbah QLD 4744

isaacregionalcouncil isaacregionalcouncil Isaacrcouncil
ISAAC REGIONAL COUNCIL ABN 39 274 142 600