Access Control Policy

Policy Endorsement:	Endorsement Required by Executive Management Team		
Policy Superseded by this Policy:	Not Applicable		
Directorate:	Digital Technology		
Responsible Officer:	Chief Information Officer		
Policy Type:	Discretional		
File Number:	A6566826	Version No:	2
1st Adopted by EMT	5 May 2020	Last Adopted by EMT:	19 February 2025
Review Period:	Annually	Next Review:	May 2027

TABLE OF CONTENTS

1. POLICY OBJECTIVE (OR PURPOSE)

Access Control Policy will be developed to reduce risks associated with unauthorised access to Council's Network and Information Systems.

All Council systems and information are subject to access controls to:

- To ensure effective management of access
- Limit access to information in accordance with Council requirements and obligations
- To enforce authorised access control across data and systems
- To prevent unauthorised access to data and systems
- To make staff accountable for safeguarding their authentication information

There are many influencing factors in formulating access control policies including:

- The security of the information stored and processed by the system
- Operational requirements
- Threats and vulnerabilities
- Regulatory compliance
- Contractual obligations

2. BACKGROUND

Access Control plays a significant role in securing Council's network services, data and information systems. To align with the Australian Essential 8 standard for the management of information security Council is required to develop an Access Control Policy.

Council is currently transitioning to phishing-resistant authentication. Staff will have the option to use both authentication technologies, with the expectation that traditional passwords will be phased out when technically possible.

3. SCOPE

The Access Control Policy applies to:

- **Standard User Access** - all persons accessing Council's systems, applications, network services and end-user devices that store and/or transmit information as part of their day to day role or requested by Council.
- **Privileged User Access –** specific staff that are required elevated access to undertake specific activities that are not required at all times. These users would have system administrator access and /or staff working with sensitive information.
- Staff involved in defining and managing either Standard User or Privileged User Access
- Digital Technology Staff

Third Party Contractors or Vendors who require access to Council's systems, applications and network services.

4. DEFINITIONS

Term	Definition
AD	Microsoft Active Directory
SSO	Single Sign-On

Essential 8	Best practice standards for Information Security Management

5. POLICY

Council establishes access control to improve the security of its systems and information. This helps to reduce the risk of undesired exposure of Council information and data or causing interruption to systems where this information/data is stored.

It is vital that every user share in the responsibility of protecting Council's systems by protecting their sensitive authentication information (password).

User Responsibilities

To maximise the security of our systems, every user is expected to adhere to the following:

- Use of strong passwords.
- Avoid easily guessable passwords such as their name, family members, year or birthdate.
- Never share passwords or allow others to use your account
- Never attempt to access any system with other users credentials
- Avoid reuse of Council related passwords for personal accounts
- Avoid recording passwords on paper or through email
- Ensure that any work PC or device left unattended is screen locked or logged out
- Inform Council's DT Service Desk of any changes of role or user access requirements as soon as possible
- Inform Council's DT Service Desk if you suspect your account or password has been compromised e.g. phishing, suspicious computer behavior
- When possible, authenticate with phishing resistant authentication instead of standard password authentication

Failure to comply with these requirements may result in the organisation taking disciplinary action against individual(s) concerned.

Authentication and Password security – Active Directory Services (AD)

AD is Council's means through which staff logon to Council's network. AD is also used to authenticate users to other applications. e.g. Objective, Property and Rating, Chris21 etc.

Multifactor authentication (using two or more forms of identification to authenticate a user) to access applications and/or network services remotely will be required in addition to user credentials. These include remote access via:

- Microsoft Office 365 environment
- CGD Staff Applications Portal
- VPN

Single Sign-on (SSO) will be used where supported by vendors unless the security requirements require additional logon details.

Whether single or multi-factor authentication is used, strong passwords must be enforced in all systems in accordance with Council's password standards. When possible, phishing resistant authentication should be the first preference over standard password authentication.

Password Policy Parameters

Parameter	Value
Standard User Access	
Minimum length	15 characters
Maximum length	25 characters
Re-use cycle	Cannot be the same as any of the previous 24

Characters required	Needs to meet three of the following requirements: At least one upper-case letter At least one lower-case letter At least one number At least one special character
Change frequency	12 months
Password attempts before account lockout	4
Account lockout duration	2 Hours
Account lockout action	Automatic after 2 hours or re-enabled by the DT Service Desk
Other Controls	Passwords / passphrase must not be on a list of blacklisted passwords as defined by Council/3rd party vendor e.g. Microsoft
Privileged User Access including staff involved in defining user access	
Minimum length	15 characters
Maximum length	25 characters
Re-use cycle	Cannot be the same as any of the previous 24
Characters required	Needs to meet three of the following requirements: At least one upper-case letter At least one lower-case letter At least one number At least one special character
Change frequency	12 months
Password attempts before account lockout	4
Account lockout duration	2 Hours
Account lockout action	Automatic after 2 hours or re-enabled by the DT Service Desk
Other Controls	Passwords / passphrase must not be on a list of blacklisted passwords as defined by Council/3rd party vendor e.g. Microsoft
Information Technology Staff	
Minimum length	15 characters
Maximum length	25 characters
Re-use cycle	Cannot be the same as any of the previous 24
Characters required	Needs to meet three of the following requirements: At least one upper-case letter At least one lower-case letter At least one number At least one special character
Change frequency	12 months
Password attempts before account lockout	4
Account lockout duration	2 Hours
Account lockout action	Re-enabled by the DT Service Desk or self-service mobile application
Other Controls	Passwords / passphrase must not be on a list of blacklisted passwords as defined by Council/3rd party vendor e.g. Microsoft
Third Party IT Contractors or Vendors	
Password	Set by DT staff
Change frequency	never expires - manually managed
Account lockout	Manual based on dates
Account lockout action	Re-enabled by the DT Staff
Other Controls	Passwords must not be on a list of blacklisted passwords as defined by Council/3rd party vendor e.g. Microsoft

Access Control in System and Applications

All Council systems and applications used to process, support and store Councils information must support secure access controls. In order to deliver this the following requirements must be considered:

- Ability to create individual user accounts
- Ability to define roles or groups to which users accounts can be assigned
- Support access permissions (e.g. read, write, delete, execute) to system/applications objects (e.g. files, programs, menus) to user accounts roles or groups.
- Ability to provide various levels of restricted access
- Ability to administer user accounts including enable and disable
- Ability to maintain security auditing facilities including, logon/logoffs, unsuccessful logon attempts, and account administration activities stored for 30 days minimum and the logs communicated to Security Information and Event Management (SIEM) platform.
- Active directory integration, if no integration is possible – application passwords must best match corporate policy (e.g. GoldCare)
- Session management Active directory integration, if no integration is possible – application passwords must best match corporate policy (e.g. GoldCare)

Access provided to utility programs that may provide a method of bypassing system security (e.g. data manipulation tools) must be strictly controlled and their use restricted to identified individuals and specific circumstances e.g. as part of security/penetration test arrangement.

Access Control for Cloud Environments

When establishing new Cloud based applications/solutions the following access requirements must be considered:

- Ability to integrate with Councils Active Directory service (SSO) this is a mandatory requirement
- Ability for manage user access, roles and responsibilities
- Integrate with Council's Electronic Documents Management system (EDRMS) for the storage of documents
- If Active Directory integration is not supported (legacy applications only) application passwords must best match corporate policy

Access Control for mobile devices (Phones/tablets/etc.)

Access control for a device will have a four- or six-digit code or biometric input will form part of the multi factor authentication (applications will still require AD or phishing resistant authentication in addition to device authentication).

6. RESPONSIBILITIES

The IT department (Digital Technology) is responsible for implementing and maintaining the access control policy to ensure the security of Council's systems and information. This includes configuring and managing user accounts, enforcing strong password policies, and ensuring multi-factor authentication is in place for remote access. The IT department must also monitor and audit access to systems and applications, promptly address any security incidents, and provide support to users in adhering to the policy. Additionally, the IT department is tasked with integrating access controls with the Council's Active Directory service and ensuring that all systems and applications comply with the established security standards.

7. REPORTING, MONITORING AND REVIEW

To ensure the standards of this policy are met, Digital Technology will measure, conduct regular audits and assessments and monitor compliance with security protocols and identify potential vulnerabilities. Incident reporting mechanisms will be established, enabling staff to promptly report security breaches or suspicious activities. The success of the policy will be reviewed through periodic evaluations, including analysis of incident reports, audit findings, and feedback from users.

8. REFERENCES AND RELATED DOCUMENTS

- Information Security Policy
- Mobile Device Policy
- *Privacy and Data Protection Act 2014*