**Text

Description automatically generated with low confidence**

**Council password policy [Template]**

|  |  |
| --- | --- |
| **Title:** Council password policy | |
| **Council name:** Council Name | **Version:** 1.0 |
| **Approved by:** | **Approval date:** |
| **Senior management approval:** | |
| **Effective date:** | **Last updated:** |
| **Author:** | |
| **Scope**  The scope of this policy applies to all council employees, contractors, volunteers, vendors, agency staff and partner agencies who:   * store any non-public Council information * have or are responsible for any Council network account or resources (or any form of access that supports or requires a password) * have access to the Council data network * store or process any Council personal, sensitive or confidential information. | |
| **Purpose**  The purpose of this password policy is to establish the framework for administering passwords for the council as part of its efforts to maintain the confidentiality, integrity and availability of information. | |
| **Responsibility**  The <IT. department> of Council Name council is responsible for administering, maintaining and updating this policy with the approval of management. | |
| **Objectives**  The objective of this policy is to provide secure and appropriate access to Council Name council’s applications, and to Council Name council systems and data used, processed, stored, maintained and/or transmitted in and through those information systems. | |
| **Strategy and focus**  Council Name council 's primary access control objective is to ensure that access to Council systems, networks, applications and data is only granted to council employees and other authorized individuals where required for the performance of their work. The focus of access control is to define the responsibilities of Council Name council employees and other authorized individuals in promoting secured and appropriate access to all council systems and IT resources. | |
| **Policy**  Council Name council is committed to securing all council information stored or accessed through Council Name council computers or networks. Access to computer systems is restricted to those employees and nonemployees authorized for such access, and who have been issued appropriate unique user IDs and passwords. Council Name council considers passwords to be highly confidential. This policy will not exclude the use of other access control mechanisms such as biometrics (e.g., fingerprints or retina scans), proximity cards (special identification cards) or technology which allows users to reset their own passwords.  Council Name council will implement, whenever feasible, SSO, hardware tokens and biometric solutions to applications, networks and other resources to ease compliance with this policy. IT security teams will evaluate password managers and determine the priority, steps and scheduling for implementation of these tools.  All council employees and managers are responsible for complying with this policy. Any individual attempting to or requesting someone else to circumvent security or administrative access controls is in violation of this policy.  All users of Council Name council systems and services are required to adhere to the following rules to use, access, store, process and/or display data acquired from council-owned applications and systems. In addition, contractors and their associated employees and agents must adhere to and agree with the following rules:   1. Access to Council Name council owned applications and systems is granted solely to conduct legitimate business on behalf of the council. 2. Access to specific system functions and data resources is consistent with each user's scope of employment and job responsibilities. 3. Access requests, including user IDs and passwords, via agreed council approval processes, with all access requests being approved by a separate, authorised manager. 4. Access requests for department users must be approved by applicable council department personnel. 5. User accounts will remain active until a user's employment relationship either changes or terminates, or a period of non-use (<specify time period>) is exceeded, after which the account will be disabled. 6. Managers are notified of all access changes for their users. 7. All contractors and their associated employees and agents must read, agree and sign the appropriate forms before access to Council Name council networks and/or systems is permitted, and must adhere to the policies set forth in this document. 8. All requests for new access, changes to existing access or termination of access must be submitted with management approvals and justifications if needed, following agreed Council procedures. 9. Council Name council’s <help desk> shall be contacted with all requests for access activities, e.g., user ID and/or password requests and/or changes. | |
| **Password guidelines**   1. Use multi-factor authentication (MFA) for all important accounts such as administrative users, and internet-facing systems. 2. Use alternatives to passwords such as SSO, hardware tokens and biometric solutions if possible. 3. Passwords must be a minimum of <specify number> characters. 4. When an initial password is created for a new user ID, or reset, an individual must change the password at the next logon for applications which enable user-initiated password changes. 5. For applications that don't support automatic password changes, users are responsible for initiating the change as above. Exceptions are permitted for automated systems (applications, etc.) that communicate without human interaction (computer-to-computer communication). 6. Separate passwords should be used for email; email passwords must be different to all other passwords. 7. Use 3 random words to create a strong, unique password that you will remember. 8. Passwords should not automatically expire; only change passwords on indication or suspicion of compromise. 9. Passwords should be saved in browsers or password managers whenever possible to help in not forgetting them and to protect from fake websites 10. User IDs and passwords or open computer application sessions should not be shared. 11. Screensavers with passwords should be used for desktop computers and should be activated after no more than <specify number> minutes of inactivity. 12. Terminals in high-traffic or public areas or with access to confidential information should employ automatic logoff or screensavers with much shorter periods of time (typically <specify number>).   **Do not:**   * reveal a password over the phone to ANYONE * reveal a password in an email message * reveal a password to the boss * talk about a password in front of others * hint at the format of a password (e.g., "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 leave * write passwords down and store them anywhere in your office. * store passwords in a file on ANY computer system without encryption. | |
| **Password administration**   1. Failed login attempts may be recorded and reviewed for follow-up action. 2. Password systems should be configured with throttling to restrict the number of failed login attempts. 3. Access privileges will be reviewed prior to granting access based on factors including job title and function (role-based access) or the individual (user-based access). 4. User IDs, passwords or email accounts are not to be shared or transferred to another individual. This includes avoiding shared user accounts, such as Admin1, or Helpdesk. All actions should be attributable to a named, unique account. 5. New accounts may be obtained by calling <IT. Management>. Approval is required before any account can be created. | |
| **Noncompliance with this policy**  Council Name council employees and authorized contractors who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures as may be determined by Council Name council 's human resources. | |
| **Management review and audit availability**  Council Name council management will review and update this policy on a <annual basis>. As changes to council policies are indicated, Council Name council management may initiate a change management request to alter the policy (or policies). All council policies will be available for review during scheduled audits. | |