https://communityds.com.au
1800 503 981
PO Box 134
Unley, SA, 5061

Password & User Account Policy

Protect customer data by applying strong authentication methods

1. Abstract

The password and user management policy is designed to protect the privacy of client data from unauthorised access, and is a key part of Community Data Solutions commitment to data security.

2. Revision history

Current as of: 30 May 2023

- Version 1.2

3. Overview

Community Data Solutions User Accounts must be protected by effective passwords. An effective password is both strong and difficult to guess by manual or automated means. Strong passwords have a minimum length and are composed of letters, numbers and special characters. It is also important that they are not based on common dictionary words (see the Password Guidelines section below). The use of passphrases as a secure alternative to password is recommended.

Community Data Solutions offer a Multi-Factor-Authentication method to all users. Using an additional authentication process ensures that users apply the best available protection of their account. While MFA is not mandatory on CDS systems, it is strongly recommended.

4. Scope

This policy applies to all users of Community Data Solutions products.

5. Policy

Account holders who use Community Data Solutions (CDS) managed products are responsible for all activities associated with their accounts and the information entered into, or extracted from these products. Each licensed user is responsible for their use of technology including the device type and location used to access CDS products.

The integrity and secrecy of an individual's password is a key element of that responsibility. The older a password is, the higher the probability is that the password has been compromised, e.g. a silent compromise incident where the password

entered was tracked or shared with others. If you are not careful with your password, significant damage known as a Data Breach may be caused to your organisation and the clients serviced.

Having an adequate password policy is a step that entities are required to take under the Privacy Act 1988 (Cth) (Privacy Act) to protect the personal information they hold.

5.1 Implementation

5.1.1 Account holders must:

- Create a strong password (see the Password Guidelines section below).
- Change their password at least once a year to reduce the risk of a password being discovered.
- Safeguard their password. For example, users must not write down their password on paper or store the password on a computer or phone where another person can access it.
- Ensure the browser used to access the CDS product does not remember the password. Please discuss ways to remove passwords from the browser with your system administrator or CDS support team.
- Never share their password with anyone inside or outside of their organisation.
- Never reuse their password for any other service.
- Change their password immediately if there is any chance that it has been guessed, stolen, intercepted, or otherwise compromised.
- Report any incidents of unauthorised account use to their system administrator.

5.1.2 Account holders should:

- Enable Multi-Factor-Authentication method for their account.

5.1.3 System administrators are expected to:

- Enforce required password strength for all users granted access to a CDS product.
- Never store a user's password in any electronic system other than in an authorised secured password management software.
- Prevent, or take steps to reduce the likelihood of, the exposure of any clear text account passwords.
- Ensure passwords and user accounts are not shared across the organisation. Each person must have their own account and password.
- Never request that passwords be sent over an insecure communication medium like Email, SMS, Instant Messaging, Google docs or an MS Office file.
- Immediately make a user account inactive when an employee leaves the organisation.

5.2 Implications for You and your Organisation

New strategies are constantly being created to break through security measures. Considering the sensitive and private information managed via CDS products it is essential that all users are educated of the risks and the best practices available to reduce that risk. CDS will revise this policy from time to time and communicate any changes to its customers. Ultimately, account security depends on users following the password policy to prevent unauthorised use of accounts.

CDS incorporate processes to enforce password and account management standards. This means that at initial account creation and on password update, passwords will be tested and weak passwords be rejected.

As of November 2022, in order to reduce the risk of unauthorised login, any user account that has not been accessed in the last 12 months must change their password using the product's password recovery tool to regain access to the product.

5.3 Password Guidelines

Community Data Solutions recommends following password generation guidelines as discussed in the password protection article on Wikipedia. Please also consider the below recommendations.

5.3.1 Basics recommendations:

- Avoid using words found in dictionaries, English or foreign.
- To help make a secure password that you can remember, try and think of a passphrase. For example: “sWimmingwIth21cAts” is an 18 character password that uses three different character classes, lowercase, uppercase and numeric, but is easy to remember.
- Avoid using passwords based on personal information such as: name, nickname, birthdate, spouse's name, pet's name, friend’s name, hometown, phone number, address etc.
- Never use a password based on your username, account name, computer name or email address.
- Ensure that no one is looking over your shoulder while you are typing your password.

6. Policy enquiries contact information

Please submit all inquiries to Community Data Solutions’ Chief information security officer via email: security@communityds.com.au