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

Data Security Information

1. Abstract

Community Data Solutions security information sheet identifies both the security services delivered and the security measure employed to protect customer data.

2. Revision History

Current as of: 15 June 2021

- Version 1.1

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

Data Security Information

Summary

The term “Data Security” can mean many things to different people so this information sheet outlines how Community Data Solutions (CDS) ensures the highest levels of data security for customer data.

Physical Security

CDS only uses trusted and Australian Government approved service providers to host its products and all data centers are located in Australia so we can ensure data sovereignty.

The data centres used by CDS comply with the Australian Signals Directorate (ASD) Information Security Manual (ISM) and has the following certifications; IRAP, CSA, ISO 9001, ISO 27001, ISO 27017, ISO 27018, PCI DSS Level 1, SOC 1, SOC 2, SOC 3, General Controls Report. Other customers in the data centres include Australian Government agencies.

Security of Data Access

Any database solution needs to ensure that only appropriately authorised people have access to the data necessary to complete their work. CDS databases can only be accessed with a valid Username and Password and each Username is allocated to specific Roles within the database solution which determines the extent of client data they can access, view, edit and delete. This authentication process ensures only authorised Users have access to data for their required Role(s) within the organisation. Managers within the organisation can utilise the “Manage Users” capability to create/deactivate Users, change passwords and assign Users to specific Roles. Users can also apply the recommended Multi-Factor Authentication method available to further protect their account.

Security of Data Transmission (TLS)

All Community Data Solutions databases provide high level, industry standard, Transaction Layer Security (TLS) encryption of data transmitted between a user's web-browser and our servers. This is the same level of security used for online credit card transactions. You can verify all data is being transmitted securely by looking at the address bar in your web browser. All web page requests are redirected to “https://” which uses the TLS protocol.

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

Backing Up Data

Regardless of how well designed and managed a particular database solution is, there is a potential for failure of hardware (e.g. hard disk drives) and the loss of data. In order to mitigate this risk, all CDS products, databases and files are frequently backed up. This ensures that in the event of server failure, we can always access and recover data from the most recent backup.

Additionally, every night, a snapshot of the database is generated and securely transferred to a separate system. This ensures that if a critical failure completely impairs a data centre, we are still able to retrieve the data and restore it.

FAQ

Can we receive a full copy of the database?

Yes, you can request a full copy of your database via our support help desk. Charges may apply. You can also request a daily backup of your database for an annual fee.

Who owns the data we enter into the database?

You, the client, own the data. CDS is simply a custodian of that data on your behalf. Should you opt to terminate CDS service, you will receive a copy of your data and all copies managed by CDS will be destroyed.

Where is your data stored?

In order to meet our obligations under the National Privacy Principles, all data is stored in Australia.

How is authentication performed to gain access to the system?

CDS provides mandatory password authentication and optional Multi-Factor Authentication MFA service.

How can the system be accessed?

All CDS systems are accessed via a web browser. Users must ensure their web browser is up to date with the latest security updates. All current browsers are supported. CDS reserves the right to prevent access to out of date or insecure browsers.

Are CDS systems audited for security vulnerabilities by a 3rd party?

All CDS systems are subject to an annual penetration test conducted by a certified 3rd party auditor.