communityds.com.au
1800 503 981
1-F 214 Greenhill Rd
Eastwood, SA, 5063

Data Security Information

1. Abstract

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

2. Revision History

Current as of: 11 September 2025

- Version 1.2

communityds.com.au
1800 503 981
1-F 214 Greenhill Rd
Eastwood, SA, 5063

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) ensure 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 centers 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 centers 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 should also implement 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 that 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.

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.

communityds.com.au
1800 503 981
1-F 214 Greenhill Rd
Eastwood, SA, 5063

Additionally, every night, a snapshot of the database is generated, encrypted and securely transferred to a separate location known as availability zones. This ensures that if a critical failure completely impairs a data center, 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 to 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?

Your data and all our services are hosted in the Amazon Web Services (AWS) Sydney with backups distributed to different Availability Zones within Australia. CDS uphold Australian data sovereignty as a mandatory KPI.

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.

How is authentication performed to gain access to the system?

CDS applications support username and password authentication method and provide an optional, recommended Multi-Factor Authentication MFA service. We are also able to restrict access to our systems to computers linked to your office network; this can reduce risk of unauthorised access. CDS monitor all user access to systems and applications and will lock user accounts subject to suspected unauthorised login attempts.

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.

Does your organisation have defined and published an information security policy that covers the to be provided service?

CDS has an information security policy that covers access and usage of customer information and internal resources. Our policy is private, but we can provide extract of relevant sections to address specific questions.

Has CDS appointed and deployed an information security officer (ISO/CISO) who is responsible for security management that covers our service including incident handling, service availability and business continuity?

Aviv Efrat is our Chief Information Security Officer (CISO) reporting to Tom Twelftree CEO. Please send all security information questions and requests to: security@communityds.com.au

communityds.com.au
1800 503 981
1-F 214 Greenhill Rd
Eastwood, SA, 5063

Does CDS have a dedicated function/person responsible for ensuring compliance with applicable data privacy laws and your internal data privacy policy?

Aviv Efrat is our Chief Information Security Officer (CISO) reporting to Tom Twelftree CEO. Please send all compliance and data privacy information questions and requests to: security@communityds.com.au

Has CDS implemented an information security management system (ISMS) that is aligned with one or more industry standards or frameworks that covers the to be provided service?

CDS has a comprehensive security program that is built around compliance with ISM - Australian Government Information Security Manual. ISM manual covers ISO27001 controls with additional controls specific for Australian security context. ISM security framework is updated on a regular basis, as such, providers are rarely able to be fully certified, and any certification obtained at a given point in time is temporary.

At this point in time, CDS is not certified by an ISO27001 auditor, however we comply with most of ISO27001 controls, and our entire infrastructure is hosted on AWS Australia which is fully certified for ISO27001, NIST and more. Please read the following resource for more information. https://aws.amazon.com/compliance/.

Does CDS have a written data privacy policy (i.e., an internal company policy that documents requirements on how to handle and protect personal data and to which employees are bound to comply)?

CDS has a public privacy policy you can access via our website or the link below.

https://communityds.com.au/wp-content/uploads/2021/06/PUBLIC-CDS-Privacy-Policy.pdf

Do all employees receive privacy trainings at least annually?

CDS employees are required to undertake an annual online security awareness training that covers both privacy legal requirements and common security attacks.

Do all employees have to sign a non-disclosure policy covering the protection of customer data?

CDS employees are bound to comply with all company policies including non-disclosure of customer data. Compliance is a condition of employment and is stated in employee contracts.

Do you conduct background checks on employees during the hiring process?

Police checks and working with children checks are a requirement of employment. All staff must undertake a National Police check and A Working with Children check in their state of residency every 5 years.

What privacy and security measures are used by CDS to protect customer data?

CDS utilises a range of technologies to secure customer data including:

- Data is encrypted when sent from your browser to our servers (at transit) and when stored in the database (at rest).
- Backup data and files regularly and encrypt data to ensure its securely.
- Enable and maintain controls to monitor and prevent unauthorised access.
- Monitor access and system logs for suspicious activities 24/7.
- Enable means to classify data entities and apply confidentiality technologies to protect PII & sensitive data.
- Secure user accounts with multi-factor-authentication.

communityds.com.au
1800 503 981
1-F 214 Greenhill Rd
Eastwood, SA, 5063

- Provide a secure file transfer service between customer and CDS system (send and receive files).

Does CDS have a vulnerability management process in place covering identification, risk assessment and remediation that covers the to be provided service?

CDS conduct a monthly security check of all code library and infrastructure components. All vulnerable components are upgraded based on vendor recommendation or disabled if vendor has no available patches. Code libraries are upgraded and tested for the relevant vulnerability. CDS uses urgency classifications to dictate vulnerability patching turnaround time.

Does CDS use subcontracts or suppliers that play a role to deliver this service and manage the risk of third-party suppliers with a documented approach.

CDS engages suppliers who adhere to Australian Privacy Laws and regulations and comply with a formal security framework. CDS only uses infrastructure and communication suppliers for service delivery and handle all other operations in-house.

Does CDS have a data breach response plan implemented that covers the to be provided service?

Yes, the data breach response plan covers various data breach and suspected data breach scenarios such as

- Loss of customer data held in CDS system
- Loss of customer data held in a 3rd party system (such as Deputy scheduling)
- Unauthorised access to client's confidential data
- Unauthorised disclosure of customer data

In the event of data breach, customers will be notified by phone call to CEO and primary contact person as well as formally via email based on our 'External Communication Plan'.

Does your organisation have insurance cover for information security incidents?

CDS has cyber insurance renewed on annual basis.