cognise.

Security FAQ

Security

Cognise runs entirely on the trusted industry-leading cloud service provider Amazon Web Services (AWS). We use AWS for a variety of reasons; trust, security, and reliability being top of mind. AWS's security policy is published here:

https://aws.amazon.com/security

What security provisions and practices are in place at your data centre(s)?

AWS data centre facilities feature 24-hour manned security, biometric access control, video surveillance, and physical locks.
All systems, networked devices, and circuits are constantly monitored.

Is our data encrypted?

All communications with and between Cognise servers are encrypted using industry-standard TLS/SSL.

What security certifications do you or your vendors have?

- AWS facilities are accredited under: ISO 27001, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- IRAP
- Privacy Act (New Zealand and Australia)
- And others. More from AWS: https://aws.amazon.com/compliance

Does your company outsource any portion of your information security?

Cognise relies on industry-leading vendors like Google, Amazon and Microsoft to provide services like application hosting, corporate email security and corporate file security.

Does your company have a program in place to periodically test security controls?

Cognise is currently developing a program to periodically test security controls. This page will be updated as the program develops.

Who owns our data?

Your content is owned by you, and only you choose with whom to share your data. Learning objects are owned and managed by the creator.

How is data backed up?

Cognise utilises Database Backups every 12 hours and content replication once a day. All Data is backed up to an offsite location daily.

Where is our data stored?

Cognise runs from AWS's data centre located in Sydney, Australia and utilises some services in Oregon, USA which are not available in Sydney. These services currently include SES and SNS (used by SES). We also run Cloudfront distributions which are available globally.

Who has access to our data?

Only Cognise administrators and customer/technical support managers have access to your learning data and records. Our staff will not grant access to third parties or otherwise disseminate your learning data without your permission. If there is a request for support, or if you hire our consulting services, then the person assigned to the request may, with your permission, log into your account for the purpose of troubleshooting and correcting the reported issue or performing the requested task.

The policies and practices of Cognise, and of the Amazon Web Services platform on which Cognise is hosted, are consistent with the objectives of the Health Insurance Portability and Accountability Act (HIPAA) with regard to data security and data privacy.

Data Privacy

In the following limited situations, we may disclose information that we collect or that you provide to us

- To our contractors, service providers and other third parties we use to support our business and who are obligated to keep personal information confidential and use it only for the purposes for which we disclose it to them.
- In an aggregated or anonymised format where no individual can be identified or linked to any part of the information.
- To comply with any court order, law or legal process, including responding to a governmental or regulatory request.
- To enforce our rights arising from any contracts entered into between you and us and for billing and collection.
- To a buyer or other successor in the event of a merger, sale or transfer of some or all of Cognise's assets.
- For any other purpose disclosed by us when you provide the information.
- With your consent.

We only use information that we collect about or from course takers, including any personal information, to:

- Improve our Services and resolve technical issues.
- Provide customer feedback and support.
- Fulfil any other purpose for which you provide it.

Do you guarantee full erasure of data?

A formal written request needs to be made and may incur charges. Deleting your content may not immediately remove the content you have published from our systems, because of caching, backups, or other references to your account. Cognise guarantees full erasure of deleted data within 90 days of a written request.

Cognise's Privacy Policy is here:
https://cognise.co.nz/privacy

Amazon's - AWS in the Context of New Zealand Privacy and Data Protection considerations:
https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_New_Zealand_Privacy_Considerations.pdf

https://aws.amazon.com/compliance/new-zealand-data-protection/

Availability

What is your uptime?

Cognise's availability is consistently above 99.9.

What practices / controls are in place to maximize uptime?

Cognise runs in facilities powered by redundant power, each with UPS and backup generators. Amazon's application deployment model minimises the risk that changes to the Cognise application will disrupt service.

The Cognise infrastructure is highly automated and any services can be rebuilt in a matter of hours in the event of catastrophic system failure.

How is planned downtime scheduled?

Our deployment platform usually obviates the need for downtime when we make changes to Cognise. If we do require downtime it will usually be less than 5 minutes and done outside of normal business hours. If we plan downtime we will notify customers by email at least 24 hours in advance.

Access Control

What controls are in place to manage access to Cognise applications and infrastructure?

- Internal access to Cognise servers is controlled within a secure VPC and all authentication is managed by ssh keys.
- All user access to Cognise is governed by access rights, authenticated by username and password, or SSO services provided by the customer. Multi Factor Authentication is also available as optional or compulsory for users.
- If passwords are used they are always encrypted, never stored as plain text.

What controls are in place to keep a customer's data separate from other customers?

- Cognise's application security architecture ensures all data is partitioned and accessed by strict scopes to ensure data is not shared.
- We also offer managed instances of the Cognise platform to completely isolate customer data. Contact our sales team to talk about a custom SLA.

cognise.

Learn more

www.cognise.com

Let's Chat

+64 4 978 7101

Product & Company

Founded in 2013, Cognise is easy-to-use learning software for success focussed organisations that need to effectively manage workplace capability.

Cognise is a SaaS product of the **allfields** group of companies, a well-established technology company and leader in corporate change management and digital learning. Cognise is used in small, medium and large workplaces, and successfully in large tech rollouts involving thousands of end users.