THINKING BOARD EVALUATOR

POWERED BY INDEPENDENT AUDIT

THINKING BOARD® EVALUATOR- IT/SECURITY INFORMATION

Infrastructure

We use Amazon Web Services ("AWS") to power everything that Thinking Board has to offer. As a Thinking Board customer, you inherit all the best practices of AWS policies, architecture, and operational processes.

Amazon Web Services is considered the industry leader in cloud services and is trusted by organisations all over the world.

Amazon's secure data centres enable the redundancy and scaling that equates to a secure and reliable service for Thinking Board databases.

- **Compliance** - AWS environments are continuously audited, with certifications from accreditation bodies across geographies and verticals. Amazon has achieved compliance with the strictest compliance programs.
- **DDoS Mitigation** - AWS provides a robust platform that is not only pre-built to mitigate some attacks, but it also allows us to react quickly to spread out impact if there is an attack.
  We have also added safeguards to underlying servers as an additional level of protection.
- **Geographic Distribution** - Amazon operates data centres all over the world, adding redundancy and scaling to your data and backups.
- **SOC 3 and ISO 27001 Certified** – Thinking Board is automatically certified for many stringent security standards by using AWS as its infrastructure.
- **Firewalls** - We use firewalls to protect every virtual server, database, and load balancer to ensure that only authorised traffic is accessing those resources.

Encryption

We encrypt all data within Thinking Board. This includes all personal data and sensitive client data. Any encrypted data must be *decrypted* in order to be read. By encrypting your data, we ensure that only authorised parties can read it.

- **Encryption in transit** – We encrypt all data as it moves between our servers and your web browser. The Platform uses TLS (256-bit encryption) when being accessed via the browser, over HTTPS
- **Encryption at rest** – We encrypt all data that's stored on our servers. The platform uses AES 256 encryption for the database, this includes all data in all our databases and back-ups.

Backups

All data within Thinking Board is backed up with several layers of redundancy.

The Server

Automatic snapshots of the production server are taken daily and stored as backups at AWS EC2 cloud. We keep 14 days of backups in the EU Ireland availability zone.

In addition, the last backup volume of each week is copied to EU Frankfurt availability zone.

We keep 14 days of snapshots history at EC2 Ireland Availability zone and 2 months history of weekly snapshots at EC2 Frankfurt Availability zone. Volume snapshots are easy and fast to restore using standard AWS console commands.

The Database

In addition to the volume snapshots backup, we also have a database backup procedure. If for any reason AWS snapshots cannot be restored, we can recover all data using these backups. Database backups are taken daily and stored at S3 storage in Frankfurt Availability Zone. After 3 months Database backups are automatically deleted.

In the event of system failure, in most cases we would be able to relaunch Thinking Board® using the volume snapshots. However, if this is not possible then we can

recover the entire system by using the database backups together with source code backups stored both in IAL's Github account, and backed up to IAL's S3 cloud storage.

Policies

Security doesn't stop with infrastructure. Without the right polices around privacy and access, your data can still be susceptible to human error or compromise.

We allocate the same amount of attention to the people and policies responsible for running that technology as to infrastructure and technology itself.

We have carefully implemented security policies around your data's privacy and about how the Thinking Board team can access that data.

Privacy

We maintain a Privacy Policy that outlines our commitment to respecting your privacy and the privacy of the information in your account. Ultimately, the data in your account is not accessible to anyone, unless you make it accessible.

Data Ownership

Please refer to your Thinking Board SaaS Subscription Agreement for more details on Data Ownership.

Release management

We are always looking for ways to improve the user experience of Thinking Board and from time to time release new features onto the Production site. To ensure the integrity of Thinking Board we have implemented a strict Development Framework.

Our Platform development framework consists of 4 separate instances of the Platform, DEV, TEST, QA and PROD. New features go through the following development process:

- Any change to the code base is initially carried out by one of our developers in our DEV. environment.

- Once development of the new feature is complete it is moved to a TEST. environment where an in-house tester checks the code for errors.
- Once approved by the development team it is moved to a QA environment where a member of IAL tests the new feature. Once tested and verified, the development task status is changed to “approved” by the Product Owner in our development management tool.
- The new development is then scheduled into a release.
- Final approval is given by the Product Owner for a release of new features to go into Production.

New releases are performed using Teamcity for automated deployment. Access to perform changes to the code is strictly limited to two named users and is controlled with password, 2 factor authentication, and is limited to one IP address.

Maintenance and new releases are made through the AWS management consol. All changes are logged. Access is limited to two named senior developers and is controlled via 2 factor authentication. Access is only permitted through a limited IP range.

Testing

Penetration testing Thinking Board is undertaken by a Crest accredited external 3rd party at least once annually. All vulnerabilities are addressed.

A copy of the summary report of the last test can be made available upon request.

We also continually monitor and self-assess our own security. We perform regular security scans using Netcraft and use cyberlytic to perform additional scans.

Our developers regularly review the server's configuration and install all recent patches of OS and other software issued by vendors.

We use SeriLog to keep an Audit Log of all actions taken on the Platform by all users. Logs are typically only retained for 90 days.

Have Questions?

Contact support@thinkingboardevaluator.com