April 2025

Data security at Xonboard

How Xonboard ensures your data and your clients data is safe

xonboard.com.au

The kind of data that Xonboard deals with is highly sensitive, personally identifiable information. This includes data such as tax file numbers, bank account details, documents and contact information. If this information was stolen then it could be used to impersonate an identity which could then be used to access bank accounts or superannuation funds. This document outlines the methods and technology that we use at Xonboard to protect the data about employees that are onboarding.

Security standards

Xonboard (via SuperAPI) is an approved Digital Service Provider (DSP) with the Australian Tax Office (ATO). The ATO requires all DSPs to pass an initial assessment of the ISO standards, including a binding confirmation of our self certification with ISO27001.

As a significant provider as an ATO DSP, Xonboard is currently pursuing the IS27001:2013 and ISO27001:2022 security frameworks with a goal to have these in place by late 2025.

These frameworks provide a robust set of controls that ensure an organisation has a security posture that is standardised to the IT industry. While Xonboard has not been audited as conforming to the ISO27001 framework we have implemented a number of the controls, particularly around securing our system against online threats.

Security beyond ISO27001

Alongside implementing the best practices in ISO27001, we also go above and beyond the controls in the standard. We also implement additional security measures based on industry lessons and best practices.

Security control overview

Data management

- All data is held within Australian borders
- Third party access to data, e.g. for crash analysis, analytics and logging is anonymised before being sent. We have a policy of self-hosting tools where it is feasible.
- Backups are created via multiple systems. We have the ability to rollback to any moment in the previous 24 hours. We take backup snapshots every eight hours and store them in two redundant systems plus secure local storage.
- Data is always encrypted at rest and in transit. Data is encrypted in transit even in an environment that we control and has no public facing access.
- We comply with holding data in accordance with Australian standards.

- We have a data access policy available upon request.

Infrastructure

- We use Amazon Web Services (AWS) to host our systems.
- All systems are monitored for authorised and unauthorised access.
- We use code to manage our infrastructure.

Service availability

- We aim to provide 99.9% uptime. Uptime status can be viewed online at https://status.xonboard.com.au
- In the event of a total outage, we aim to restore access in four hours or less.
- We have a disaster recovery plan available upon request

Security governance

- We have a third party data access policy available upon request.
- We have a dedicated Chief Security Officer.
- We are a registered Digital Service Provider (DSP) with the ATO.

Security control

- Developer code commits are signed for integrity.
- We manage system access using Google GSuite.
- We have a policy to use 2FA (if available) on all 3rd party services that we use.
- Users will be notified of any data breach within 24 hours.
- We automatically monitor for and patch any security vulnerabilities in 3rd party libraries that our software relies on.
- We perform an annual penetration test of our software. The results of this test are available upon request.

Human resources

- All developers are located within Australia.
- All employees of Xonboard have undergone rigorous background checks.