

MYOB LiveAccounts™ Security

We understand how important your business information is to you. And we understand the trust you have placed in us to ensure your business information is kept confidential, secure and backed up. This document outlines what measures we have in place to deliver that peace of mind for you.

Your data is encrypted during transmission

All communication from the browser to LiveAccounts™ is done over secure channel (Secure Socket Layer), ensuring that the transmission of data between your computer and LiveAccounts™ is not compromised. The encryption is to the level specified by the Payment Card Industry - Data Security Standard (PCI-DSS).

Your data is stored in a highly protected environment

The data is stored behind several layers of firewalls to prevent access from the internet to the data. The access to the database is strictly controlled by application certificates and personnel authorisation.

Your data is scanned and protected from viruses

The MYOB hosting environment supports a robust anti-virus regime with regular updates and constant scanning.

Your data is accessed by robust and tested applications

The applications are reviewed in accordance with generally accepted security best practice principles (Confidentiality, Integrity, Availability, Authentication, Accountability, Least Privilege and Defence-in-Depth) and recognised industry standards. These standards include, but are not limited to:

- OWASP Guide to Building Secure Web Applications and Web Services
- OWASP Top Ten Most Critical Web Application Security Risks
- Web Application Security Consortium Threat Classification

The applications are tested regularly and before any major change is released.

Your data is stored at a secure physical location

MYOB LiveAccounts™ stores the information on hardened servers in a enterprise-grade data centre. It has 24/7/365 video surveillance, strict personnel access controls, on-site security, and audits to keep the information safe.

Any visitor to the premises must be authorised, and further authorisation is required to access areas with servers, workstations, or networking equipment. As part of the strict visitor access controls, a visitor log is kept to maintain a physical audit trail of visitor activity.

Your data is backed up

All data is backed up daily to support recovery in the event of technology problems.

Your data is available only to those authorised to view it

All access to the data is username and password protected. Users will only be allowed to access data they have permission to view.

Your data is managed by stringent policies and procedures

All staff interacting with the LiveAccounts™ environment are subject to MYOB's security policies and procedures. These have been aligned with PCI DSS requirements and cover such things as:

- Acceptable Usage
- Network Design
- Logging and Monitoring
- Access Control

Independent auditing and testing

We work closely with Stratsec (<http://www.stratsec.net/>), one of Australia's strongest and most awarded information security teams to conduct regular audits and penetration tests on both the servers and application.

For more information regarding LiveAccounts™, please contact the support team at <http://liveaccounts.myob.com/support/>.