myprosperity

myprosperity Security Overview

Introduction

Our mission is to redefine the relationship between households & finance professionals so individuals can make smarter, more efficient decisions and ultimately, live the life they want to live.

A key part of that is ensuring our customers' data is secure. Read on for an overview of our security systems and practices.

Our security program is based on the concept of 'defence in depth': we build multiple layers of security controls throughout our organisation, operating environment, and product, to provide a high level of redundancy in the event of a security control failure or exploit.

Organisational Security

Building Security

myprosperity operates primarily out of an office in Melbourne, Australia where physical access is managed by electronic key cards and limited to staff only. Where our sales team operate in other locations, they do so on company issued equipment that is monitored and secured by our security team.

Personnel Security

All personnel undergo a rigorous recruitment process which includes a mandatory reference check and police check.

All workstations issued to our personnel are configured by myprosperity to comply with our security standards. They must be properly configured and updated, as well as tracked and monitored by myprosperity's endpoint management solutions, Carbon Black.

Our default configuration sets up workstations to run up-to-date monitoring software to report potential malware, unauthorised software, and mobile storage devices.

Operational Security

Hosting

The myprosperity platform is cloud based. It is hosted on Amazon Web Services (AWS) in data centres sovereign to the country we are providing the product in.

The AWS data centres are state of the art in terms of physical and network security, redundancy, fire protection, asset management, hardware decommissioning and more.

See https://aws.amazon.com/whitepapers/overview-of-security-processes/ for details.

Encryption

Data in Transit

Transmission of data is protected using HTTPS/Secure Sockets Layer (SSL) at a minimum of 128 bit encryption or higher where devices/browsers are compatible. We use TLS 1.2 protocols, AES256 encryption, whenever supported by clients.

Data at Rest

Data stored on the platform and data backups is encrypted using high level AES-256 bit encryption.

Network Security and Server Hardening

myprosperity divides its systems into separate networks to better protect sensitive data. Our network architecture is segregated by Access Control Lists (ACLs) controlling traffic flow and limiting the accessibility of data to the systems and accounts that require it.

Systems supporting testing and development activities are hosted in a separate network from systems supporting production infrastructure. All servers within our production fleet are hardened (e.g. we disable unnecessary ports, remove default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Network access to our production environment from open, public networks is restricted, with no production servers directly accessible from the Internet. Only those network protocols essential to the delivery of myprosperity's services and its users are open on our systems. Additionally, we log, monitor, and audit all system calls and have alerts in place to detect and prevent potential host-based intrusions.

Segregation of Duties

Access to production environments is restricted to a limited set of staff with levels of access based on role. Access rights are reviewed at least quarterly.

Access Control

Provisioning

To minimise the risk of data exposure, we adhere to the principles of least privilege and role-based permissions when provisioning access: workers are only authorised to access data that they reasonably must handle in order to fulfill their current job responsibilities.

Authentication

To further reduce the risk of unauthorised access to data, myprosperity employs multi-factor authentication for all access to systems with highly classified data, including our production environment, which houses our customer data. Where possible and appropriate, we use private keys for authentication, in addition to the previously mentioned multi-factor authentication on a separate device.

Password Management

myprosperity requires technology personnel to use an approved password manager. Password managers generate, store, and enter unique and complex passwords to avoid password reuse, phishing, and other password-related risks.

System Monitoring, Logging, and Alerting

myprosperity monitors servers, workstations and mobile devices to retain and analyse a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged and retained for at least two years. Analysis of logs is automated to the extent practical in order to detect potential issues and alert responsible personnel. All production logs are stored in a separate network that is restricted to only the relevant security personnel.

Regular Security Testing

We conduct daily automated security testing and scans, as well as automated and manual code analysis. myprosperity also schedules regular testing by an independent security firm which cover a wide range of security aspects, including penetration testing and network vulnerability assessments.

Data Retention and Disposal

Customer data is removed immediately upon request by the user. We hard delete all information from currently running production systems. Our hosting provider AWS are responsible for ensuring the removal of data from disks is performed in a responsible manner before they are repurposed.

Disaster Recovery and Business Continuity Plan

myprosperity utilises services implemented by its hosting provider to distribute production operations across three separate physical locations. These locations are within one geographic region but protect our service from loss of connectivity, power infrastructure, and other common location-specific failures.

Production transactions are replicated among these discrete operating environments to protect the availability of our services in the event of a location-specific catastrophic event. We also retain a full backup copy of production data in a remote location significantly distant from the location of the primary operating environment. Full backups are saved to this remote location at least once per day and transactions are saved continuously. Backups are tested at least quarterly to ensure they can be successfully restored.

Vendor Management

To run efficiently, myprosperity engages other providers. Where those provider organisations may impact the security of our production environment, we take appropriate steps to ensure our security posture is maintained by establishing agreements that require service organisations to adhere to confidentiality commitments we have made to our customers.

Notable partners include Envestnet Yodlee for access to over 600 leading financial institutions, and CoreLogic RP Data for property data.

External Validation

Security Compliance Audits

myprosperity is continuously monitoring, auditing, and improving the design and operating effectiveness of our security controls. These activities are regularly performed by our internal security team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.

Penetration Testing

We engage independent entities to conduct application-level and infrastructure-level penetration tests at least annually. Results of these tests are shared with senior management and are triaged, prioritised, and remediated in a timely manner.

Customer Driven Audits and Penetration Tests

Our customers are welcome to perform either security control assessments or penetration testing on our environment. Please contact your Partner Enablement Manager to learn about options for scheduling either of these activities.

Product Security

Multi-Factor Authentication

Multi-factor authentication (MFA), also known as two-factor authentication, is available for our partners and their clients. myprosperity recommends making MFA mandatory for all partner staff and clients (this can be done via a dedicated setting within the platform) to enforce an additional layer of security.

Roles and responsibilities

The myprosperity platform supports multiple access levels for partners and their clients. Clients in particular can control who has access to their data and what operations can be performed on their account.

Read-Only Service

myprosperity is designed to help clients and their finance professionals organise and analyse their financial world. There is no functionality to move funds in or out of any accounts.

Conclusion

Safeguarding data is a critical part of delivering a quality platform and service. We take security very seriously and are constantly evolving our standards towards better security outcomes. If you have any questions or would like more information about our security practices, please contact our Support Team.

For information about our privacy policies, visit https://myprosperity.com.au/Info/Privacy