Mentorloop
4 Regent Street
North Richmond, Vic 3000
Australia

Mentorloop Security Policy

Document Version History

Modified By	Modifications Made	Date
Tracy Powell	Refer to staff infosec policy doc	2021-10-12
Mark Reid	Updates to *Staff workstation and device security*	2020-02-03
Mark Reid	Added Customer Data Classification policy	2019-02-27
Mark Reid	Added policy on usage of portable storage devices	2019-09-18
Mark Reid	Removed *Gateway Configuration, Application Server Access, Encryption Policies, Application User Authentication* and refer to Mentorloop System Design Specification document. Added *Staff password and encryption key policy*.	2018-02-15

Data sovereignty and datacenter management

Application servers

All Mentorloop application servers are hosted by Amazon Web Services (AWS) in the applicable region. The ap-southeast-2 region in Sydney, Australia hosts app.mentorloop.com, while eu-west-2 region in London, UK hosts app.mentorloop.co.uk.

Database instances

Database instances are provisioned by MongoDB Atlas and hosted in the corresponding AWS data center.

Mentorloop is a multi-tenant cloud application. Each environment is hosted on AWS EC2 instances isolated within their own Virtual Private Cloud (VPC) as per MongoDB Atlas' security policies.

AWS is responsible for data center management, media sanitisation, physical security, and mitigation against environmental risks.

AWS is ISO 27001 certified and SOC 3 compliant:

- AWS SOC 3 Report
- AWS ISO 27001 Global Certification

Further details and documentation regarding our vendors' compliance and security posture can be provided on request.

Monitoring and management

Network access

Please see *Mentorloop System Design Specification* document.

OS maintenance and patching

Application servers run an LTS version of Ubuntu. All instances are automated to receive and install security updates regularly, and Mentorloop administrators are notified of any issues performing automated updates. Non-security updates are assessed by administrators and installed if and when they are deemed to have a suitably low level of risk.

Audit logging and monitoring

Our logging policy is to log as much as appropriate from all system components. For details, see *Mentorloop System Design Specification* document.

Implementation, development, and acquisition of information systems

The implementation of any new information systems or processes, including internal development of new platforms and the integration of third party services must be authorised by the CTO or acting CTO. If it is determined that a third party service should be tried or tested prior to recommending its implementation, real platform/customer data must not be used under any circumstances.

Information systems configuration and security policy

Administrator access and identity management

Access to the AWS administrative console is managed via IAM and restricted to Mentorloop administrators. Specific user roles and permissions are granted only as they pertain specifically to job function. This access is regularly evaluated to ensure it is retained only when necessary.

Multi-factor authentication is enforced on all AWS accounts and regular rotation is enforced for both passwords and access keys. All user and API interactions with AWS are logged to Amazon CloudTrail for forensic auditing purposes. All shell access to application instances is logged for auditing purposes. All access to the database management console is logged for auditing purposes.

Gateway configuration

Application servers are isolated inside a VPC on a private subnet. All TCP/IP ports are closed except those required for regular operation of the Mentorloop application.

Database instances are configured to only accept connections from allow-listed IPs which are restricted to the application servers and known Mentorloop staff networks.

Staff information and data security

Refer to *Mentorloop staff information and data security policy* for more details.

Customer data segregation and security

Mentorloop standard operating procedure is for customers to access the application via a shared application instance and to store customer data across shared database instances. Appropriate safeguards are in place within the application design, architecture, and review process to ensure that user data is only accessible by the users to whom it pertains.

Data classification

Access to any data collected, processed, and stored by the Mentorloop application is in accordance with the following classification strategy:

Classification	Data examples	Visible to
Critical	Personal user-to-user correspondence, including: - All in-loop content (messages, files, events, tasks) - The "message" field of a mentoring match request - The "message" field of a mentoring match rejection	- Strictly visible only to its senders and intended recipients
Restricted	- Detailed user activity logs, ie, system & application logging	- Mentorloop Support & Engineering staff
High	- User activity metadata - User survey data - Confidential profile data	- Mentorloop Support & Engineering staff - Program Coordinators
Medium	- Public profile data	- Mentorloop Support & Engineering Staff - Program Coordinators - Program Users
Low	Aggregated/anonymised profile, program usage and survey data; strictly non-personally identifiable information.	May be shared publicly, ie, for promotional/marketing purposes.

Backups and disaster recovery

Database snapshots are taken at six-hourly, daily, weekly, and monthly intervals and stored by MongoDB Atlas in the applicable AWS data centers. Access to backups is restricted to Mentorloop administrators and can only be accessed via multi-factor authentication.

Database rollback procedures are tested regularly to ensure they can be reproduced in production environments in case of disaster.

For more details, see *Mentorloop Business Continuity & Disaster Recovery Plan*.

Incident response and disclosure policy

See *Mentorloop Security Incident Response Plan*.

Vetting and auditing of third party vendors

Prior to integrating with or using the services of third party vendors and SaaS products, Mentorloop audits the security and privacy policies and security compliance position of vendors to ensure they comply with Mentorloop's own information security posture. All vendors must agree to inform Mentorloop in writing of any changes to their security and privacy policies or compliance status, at which point further auditing is conducted to ensure that Mentorloop is still able to maintain its information security posture.

Vetting of employees

- Best practice in checking previous employment history is carried out.
- Employment history is cross checked via public methods (e.g. LinkedIn Profiles, GitHub account history) and private (direct communication with employers).
- A minimum of two references are checked, these may or may not be those provided by the candidate.
- Candidates are given an opportunity to respond to any information gathered during the vetting process.
- A number of questions concerning information security best practice, the Spam Act 2003, data diligence processes, and mission critical deployment practices are asked of job applicants during the interview process.
- Mentorloop provides candidates with copies of its InfoSec Policy, Data Storage Policy, Disaster Recovery Policy and Privacy Policy pre-second interview, questions and commentary on these policies then forms part of the second interview content.
- Where an appointment must be made before reference checks are complete, the letter of appointment specifies that it is 'subject to satisfactory vetting'.