Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Mentorloop security policy

Introduction

This document describes the security policies at Mentorloop to ensure the confidentiality, integrity, and availability of applications, processes, and systems that process Mentorloop and customer data.

Organization

Mentorloop is a leading provider of mentoring software solutions, dedicated to fostering meaningful connections and professional development opportunities. Our organization specializes in facilitating mentoring programs for businesses, educational institutions, and non-profit organizations worldwide. With a commitment to innovation and security, Mentorloop empowers individuals and organizations to achieve their goals through structured mentorship experiences, supported by cutting-edge technology and a focus on privacy and data protection.

Privacy

Mentorloop is GDPR-compliant, with more detail available in this article: GDPR - How We've Handled It. We have also published our Data processing addendum and third-party subprocessors. Mentorloop is compliant with the Australian Privacy Act (1988) including the Australian Privacy Principles (APPs). The Mentorloop Privacy Policy sets out how, as a data controller, Mentorloop collects, uses, stores, and discloses personal information; as well as how individuals can exercise rights relating to their personal information.

Data classification

Classification	Examples	Accessibility
Confidential	Personal user-to-user correspondence, including: - All in-loop content (messages, files, events, tasks)	Strictly visible only to its senders and intended recipients

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Classification	Examples	Accessibility
	- The “message” field of a mentoring match request - The “message” field of a mentoring match rejection	
Restricted	Detailed user activity, e.g. system and application logs	Mentorloop engineering staff
High sensitivity	- Participant activity metadata - Participant survey data - Participant confidential profile data	- Mentorloop staff - Program coordinators
Medium sensitivity	Participant non-confidential profile data	- Mentorloop staff - Program coordinators - Program participants
Public	Aggregated / anonymized profile, program usage, and survey data; strictly non-personally identifiable information	May be shared publicly, e.g. for promotional / marketing purposes

People practices

At Mentorloop, we prioritize the well-being and professional growth of our employees through comprehensive people practices. This includes regular performance evaluations and feedback sessions to ensure continuous improvement and alignment with organizational goals. We offer many opportunities for skill development through dedicated L&D budget and allocated time, and we provide a supportive work environment that values diversity, inclusion, and work-life balance. We enforce clear policies against discrimination, harassment, and retaliation, providing multiple channels for employees to report any concerns they may have. Our management team is dedicated to promptly addressing and resolving any issues in accordance with company policies and applicable laws, fostering a culture of trust, respect, and accountability across the organization.

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Employee screening

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. Where an appointment must be made before reference checks are complete, the letter of appointment specifies that it is 'subject to satisfactory vetting'.

Security awareness education and training

Upon commencing employment, all Mentorloop staff complete security awareness training and sign-off that they have read and agree to the Mentorloop Staff Information Security Policy. Continued training and sign-off occurs every 6 months for all staff.

Physical security

Physical access to Mentorloop headquarters is restricted to authorized personnel only. Adequate security measures, such as locks, alarms, surveillance cameras, and access control systems, are implemented to prevent unauthorized entry or theft. Physical security of all data centers is governed by the hosting provider.

Asset management

All company assets are identified and documented. Access to company assets shall be granted based on the principle of least privilege, ensuring that individuals have access only to the assets necessary for their job responsibilities. Access permissions shall be regularly reviewed and updated as needed, particularly in cases of employee transfers, terminations, or changes in job roles. Industry standard mobile device management is used to secure mobile devices.

Access control

At Mentorloop, we implement robust access control measures to safeguard sensitive information and systems. Identity and authentication protocols are enforced to ensure that only authorized individuals can access Mentorloop resources and company and customer

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

data. Mentorloop staff administrator access is secured with multi-factor authentication (MFA). Additionally, access privileges are granted based on the principle of least privilege, where individuals are only given access to the resources necessary for their roles and responsibilities. Regular audits and reviews of access rights are conducted to maintain the integrity of our access control systems and promptly revoke access for any unauthorized users. Access is evaluated during onboarding, offboarding, change of roles, and at regular intervals to ensure the proper level of access is granted.

Third-party vendors

Prior to integrating with or using the services of third-party vendors and SaaS products, Mentorloop reviews the security and privacy policies and security compliance position of vendors to ensure they comply with Mentorloop's own information security posture. Should any vendor's security and privacy policies or compliance status change, further review is conducted to ensure that Mentorloop is still able to maintain its information security posture.

Application development, maintenance, and security

All changes to the Mentorloop application require peer review focussed on quality and security as well as successful completion of automated tests, linting, and builds. Tools like Snyk and Dependabot are used to keep dependencies up to date and free from vulnerabilities. Significant changes or additions to infrastructure undergo threat modeling exercises using the STRIDE model with OWASP top 10 considered. Changes are first applied to multiple, isolated pre-production environments for testing purposes. Production data is not to be used for testing purposes. Where no alternative is available, production data must be anonymized before used for testing. Relevant application and security logs are maintained. Web application penetration testing is performed annually by an authorized and accredited third-party.

Mentorloop
4 Regent Street
Richmond, Vic 3000
Australia

Other resources

For additional information on related topics see our other policies:

- Business Continuity & Disaster Recovery plan
- Security incident response plan
- Mentorloop cloud architecture

Last updated: February 2024.