tahora

Security at Tahora

Introduction

Tahora is on a mission to create workplaces where employees belong and feel engaged. As part of this at the core of our technology strategy is ensuring data is secure and we continue to make it one of our most important responsibilities.

Our leadership team is committed to being transparent with our security policies and strategies to help all organisations and users have complete understanding and trust in our approach.

Organisational security

Tahora's security team, led by our Technology and Leadership Board, is committed to ensuring the best practices and implementation of the Tahora security programme. This includes all areas from Architecture Security, Product Security, Engineering, Operations, Detection and Response and Compliance and Risk Management.

Tahora's industry-leading enterprise security programme is centered around defending our company, your data and access to the solution from every layer. Our security programme is constantly evolving, you can find the latest information by contacting support or your customer success manager.

Protecting customer data security

Our core focus is to prevent unauthorised access to our company and user data. To ensure this is met our team of security experts work in partnership with our industry security partners and agencies to take exhaustive steps to identify and mitigate risks, whilst maintaining best practices and always striving to improve our methods.

Secure by design

Whilst we are constantly striving to catch all potential vulnerabilities before they occur, in the design and testing phases, we do understand that sometimes mistakes may happen. We are proud to have a strong process in place for how we respond to these. All identified vulnerabilities are quickly validated for accuracy, triaged, and tracked to resolution.

Encryption

- Data in transit

  All data transmitted between Tahora's clients and our service service is done using strong encryption protocols.Tahora supports the latest recommended secure cipher suites to encrypt all traffic in transit, requiring use of TLS 1.2 protocols, and AES encryption and SHA signatures between the clients and the server.

- Data at rest

  Data at rest in Tahora's production databases is encrypted using industry standard AES-256 encryption. Tahora has implemented appropriate safeguards to protect the creation, storage, retrieval and destruction of secrets such as encryption keys and service account credentials.

Every Tahora user's data is hosted by our partners on our shared infrastructure and logically separated from other customers' data. We use a combination of storage technologies to ensure all customer data is protected from hardware failures and quickly returns information when requested.The Tahora service is hosted in data centres maintained by industry-leading service providers, offering state-of-the art physical protection for the servers and infrastructure.

Network security and server hardening

For better protection of sensitive data, Tahora divides it's systems into separate networks. Systems for development and testing activities are hosted on a separate network from systems supporting Tahora's production infrastructure. All servers used for production are hardened by our network partners (e.g. disabling unnecessary ports, removing default passwords, etc.) and have a base configuration image applied to ensure consistency across the environment.

Access to the Tahora production network from open, public networks is restricted, with only a small number of production servers accessible from the internet. Only those network protocols essential for delivery of Tahora's service to its users are open. Additionally, Tahora's security tools log, monitor, and audit all system calls and has alerting in place for system calls that indicate a potential intrusion.

Endpoint security

All workstations issued to Tahora employees are configured by Tahora to comply with our standards for security. These standards require all workstations to be properly configured, updated, and be tracked and monitored by our endpoint management solution. Workstations run up-to-date monitoring software to report potential malware, unauthorised software, and mobile storage devices. Mobile devices that are used to engage in company business are required to be enrolled in the appropriate mobile device management system, to ensure they meet Tahora's security standards.

Access control

- Provisioning

  To minimise the risk of data exposure, Tahora operates with the view to always provide the least privilege and role-based permissions when provisioning access—employees are only authorised to access data that they reasonably need in order to fulfill their current job responsibilities. All production access is reviewed at least quarterly.

- Authentication

  To further reduce the risk of unauthorized access to data, Tahora 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, Tahora uses private keys for authentication, in addition to multi-factor authentication on a separate device.

- Password management

  Tahora requires all employees and contractors 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

Tahora monitors servers, workstations and mobile devices to retain and analyse a comprehensive view of the security state of its production and corporate infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Tahora's production environment are logged. Analysis of logs is automated to the extent practical to detect potential issues and alert responsible personnel. All production logs are restricted to only be accessible by the relevant security personnel.

Data retention and disposal

User data is removed immediately upon deletion by the end user or the company environment by the administrator. Tahora deletes all information from currently running production systems and backups are destroyed upon request.

Tahora's hosting providers are responsible for ensuring removal of data from disks is performed in a responsible manner before they are repurposed.

Disaster recovery and business continuity plan

Tahora retains a full backup copy of production data in a secure location. Full backups are saved at least once per day. We work with our hosting partners to ensure data is backed up and encrypted to leading industry standards.

Responding to security incidents

Tahora has internal working policies and procedures for responding to potential security incidents. All security incidents are managed by Tahora's Response Leads. In the event of an incident, affected customers will be informed via email from our customer success team. Incident response procedures are tested and updated at least annually.

Vendor management

To run efficiently, Tahora relies on sub-service organisations. Where those sub-service organisations may impact the security of Tahora's production environment, we take appropriate steps to ensure our security position is maintained by establishing agreements that require service organisations to adhere to confidentiality commitments we have made to users. Tahora monitors the effective operation of the organisation's safeguards by conducting reviews of all service organisations' controls before use and at least annually.

External validation

- ### Security compliance
  Tahora is continuously monitoring, auditing, and developing the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and Tahora's internal technology team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner.

- ### Penetration testing
  In addition to our compliance audits, Tahora engages independent entities to conduct application and infrastructure penetration tests at least annually. Results of these tests are shared with senior management and are triaged, prioritised, and remediated in a timely manner. Customers may receive executive summaries of these by requesting them from their account manager.

- ### Customer driven audits and penetration tests
  Our enterprise customers are welcome to perform either security controls assessments or penetration testing on Tahora's environment. Please contact your account manager to learn about options for scheduling either of these activities.

tahora.com support@tahora.com