SECURITY AT MENTIMETER

SECURITY WHITE PAPER

Mentimeter

Mentimeter

SECURITY WHITEPAPER

Security at Mentimeter

Mentimeter is committed to protecting user data through strong, industry-aligned security practices backed by ISO 27001:2022 certification and GDPR compliance. We rely on secure AWS infrastructure, apply robust encryption and access controls, and embed security throughout our software development lifecycle.

Our approach includes continuous employee training, regular vulnerability testing, clear incident response procedures, and a responsible disclosure program. This whitepaper outlines how we maintain a secure, reliable, and trustworthy platform for all our users.

Data Protection

Data Hosting

We are working with the **best-in-class service provider** for data storage - Amazon Web Service (AWS). Amazon's physical infrastructure is hosted and managed within their secure data centers. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards.

Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate

Customer data is stored in either EU-West-1 (Ireland) or US-East-1 (North Virginia), depending on compliance needs. Data is not duplicated across regions.

More about Amazon security & compliance can be found here (https://aws.amazon.com/security/) & here (https://aws.amazon.com/compliance/).

Data Classification

At Mentimeter, we classify data internally into four categories to support appropriate handling and protection measures:

- **Public**
    - Information approved for release to the general public and freely shareable both internally and externally.
- **Internal**

    - Information owned by Mentimeter or entrusted to it, shared with authorized individuals with a business need but not released to the general public.
- **Confidential**
    - Highly valuable, sensitive business information with protection dictated internally by Mentimeter. Access is limited to authorized individuals with a business need.
- **Restricted**
    - Highly valuable, sensitive business information with protection dictated by legal/contractual external requirements. Access is limited to authorized individuals with a business need.

For each of these classes appropriate data protection measures are defined.

It is important to notice that this classification is not applied to categorize individual pieces of customer data, but rather to help ensure appropriate protection of all data types based on their sensitivity and applicable legal or contractual obligations.

Data Retention

During the usual course of business, we collect data from different target groups, therefore we have established data retention standards that outline the measures and retention times we undertake to ensure compliance with applicable privacy laws and its principles.
Our internal documentation defines:

- what type of personal data we may process,
- what rights the target group has,
- the legal basis for our processing,
- how the personal data may be shared and used, and for how long.

You can read more about how long data is stored in our Privacy Policy.

Data Encryption

Data at rest
We use strong encryption for all data at rest, including **AES 256-bit** encryption for customer data stored in Mentimeter's production environment.

As outlined above and in our Privacy Policy, Mentimeter stores data on AWS servers (AWS Compliance). Customer data is logically separated to ensure integrity and confidentiality. We utilize ISO 27001, SOC 2, and FISMA-certified data centers managed by Amazon.

Data in Transit
All data in transit is encrypted using TLS 1.2 or higher. Additionally, we maintain an A+ rating from SSL Labs, a third-party security evaluator.

Mentimeter

Financial Data

Credit card information is securely stored with a Level 1 PCI-compliant third-party vendor Stripe.

Access Control & Authentication

Physical access

Access to Mentimeter's office premises is provided to staff individually and on a need-to-have basis. Access related events are logged with date, time, proximity card-id, door-id, access denied, or access granted. Entries are monitored by security cameras.

Access provisioning

Mentimeter maintains the **principle of least privilege**, meaning that every module (such as a process, a user, or a program, depending on the subject) must only have access to the information and resources that are necessary for its legitimate purpose such as role, job functions, etc.

Mentimeter maintains **separation/segregation of duties** to prevent error and fraud by ensuring that at least two individuals are responsible for separate parts of any task so that no single role or account can access, modify or use data without authorization or detection.

Passwords & authentication

User Passwords
We encrypt (hashed and salted) passwords to protect them from being exposed in case of a breach. Mentimeter can never see your password.
Employee Passwords
All Mentimeter employees are instructed to use a password manager, which ensures complex, unique and safely stored passwords are used. Additionally, password complexity requirements are enforced on all employee accounts from Google admin side.

SSO and 2FA are enforced wherever applicable.

Security Awareness & Non-disclosure

All Mentimeter employees (as well as consultants) must uphold and meet the requirements of Mentimeter's Security Policy, therefore every employee undergoes cybersecurity training upon joining and annual refresher training to stay up to date on best practices for data protection, secure system use, and threat awareness.

Mentimeter

As a condition of being granted access to Mentimeter's systems, repositories, and information, **all employees must acknowledge and agree to the following**:

- **Confidentiality**: Employees must maintain the confidentiality of all sensitive information, as any unauthorized disclosure could cause harm to Mentimeter.
- **Authorized Devices**: Confidential information may only be accessed and handled on Mentimeter-issued devices.
- **Proper Use**: Employees may only use Mentimeter's information and systems for work-related purposes and must not, directly or indirectly, use them for any other reason.
- **Access Expiration & Return of Assets**: An employee's access to Mentimeter's systems, repositories, and information expires upon termination of employment or at any time upon Mentimeter's request. Unless instructed otherwise, employees must immediately return all intellectual property and company assets in their possession when their access rights are revoked.

Incident Management & Reporting

We have in place and will maintain appropriate technical and organizational measures to protect personal data as well as other data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing (a "Security Incident").

Mentimeter has an incident management **process to detect, report, and handle security incidents**, which includes the following:

- **Reporting**: All security incidents must be reported immediately by employees and data processors. Failure to report will be considered a security violation and noted in follow-up reports.
- **Documentation & Action Plan**: Each incident is documented, evaluated, and assigned a mitigation plan. Relevant materials (files, logs, screenshots) must be preserved for legal or investigative purposes.
- **User Notification**: If a security incident affects a User, Mentimeter will notify them as soon as possible via appropriate channels.
- **Response Process**: All security breaches or attacks must follow a mandatory response process, especially if personal data is compromised.
- **Employee Training**: Employees are trained to report security incidents and vulnerabilities. Role-specific training is provided for Support and Engineering teams.
- **Annual Testing**: The incident response plan is tested annually to ensure effectiveness.

Mentimeter

Secure Software Development & Testing

Software Development Life Cycle

Our established and documented engineering practices ensure that we have security in mind in all stages of a development lifecycle. While no system is completely secure, we will do our utmost to minimize any type of risk.

Examples of security controls we follow throughout the SDLC:

- **Environment Separation**: Maintain distinct environments for application development, testing, and production.
- **Static Code Analysis**: Built into the CI/CD pipeline to proactively detect potential security issues in the code
- **Data Handling**: Avoid using production or other sensitive data in testing or development environments. Test data shall be protected
- **Change Approval**: Implement change control procedures, including peer review and human approval for all production environment changes
- **Code Review**: Ensure code changes are reviewed by individuals other than the original author
- **Managing Dependencies**: We have tools and processes for managing dependencies and related vulnerabilities.

Vulnerability management and penetration testing

We utilize Detectify for regular automatic **vulnerability scans**. In Detectify reports threats are classified in accordance with CVSS rating.

Vulnerability Remediation SLAs:

CVSS 3.1	**Remediation Time**
Low (0.1-3.9)	8 weeks
Medium (4.0-6.9)	6 weeks
High (7.0-8.9)	2 weeks
Critical (9.0-10.0)	2 weeks*

High and Critical Vulnerabilities Response Initiation

If the Security Team receives a report on a vulnerability that is critically threatening the security of Mentimeter infrastructure, and follows characteristics below, it shall be addressed as soon as possible.

The acknowledgement of such vulnerability and remediation action shall be initiated within 48 hours from report time, and ***patches for critical vulnerabilities should be applied within 48 hours*** *(working days)* ***after being available and tested****.*

Penetration tests
Mentimeter performs penetration testing on an annual basis. We always reach out to independent 3rd parties for performing penetration tests.

Third-Party Security & Vendor Management

Mentimeter sets strict security and compliance expectations for all vendors and third-party service providers. Vendors must meet industry security standards and undergo risk assessments to ensure they align with our security policies. Before integrating any third-party services, we conduct due diligence reviews, including security evaluations, compliance checks, and contractual agreements to protect data integrity and confidentiality.

Business Continuity & Disaster Recovery

Business Continuity

Mentimeter ensures service availability and resilience through a robust infrastructure, continuous monitoring, and proactive risk management. We implement redundant systems and automated failover mechanisms to minimize disruptions and maintain seamless operations.

Disaster Recovery

In the event of a cyber incident or system failure, we have a comprehensive disaster recovery plan, including regular data backups, secure offsite storage, and tested recovery procedures. These measures enable us to quickly restore services while safeguarding customer data.

Disaster Recovery Strategies
Our AWS backup strategy leverages **Multi-AZ deployments, automated snapshots**, and **WAL** (transaction log) backups for disaster recovery and high availability.

Database Backups

- **Hot Standby**: Multi-AZ deployment ensures real-time data replication to a fully synchronized standby instance in a different AZ. In case of failure, the standby instance is automatically promoted with minimal downtime.
- **Automated Daily Snapshots**: Daily backups with a retention of 7 days.
- **WAL** (Transaction Logs): Continuous backups enabling Point-in-Time Recovery (PITR) within a 7-day retention window.

Mentimeter

Backend components
Our backend compute infrastructure is designed for high availability and fault tolerance. All services are deployed across multiple Availability Zones (AZs) to ensure resilience against AZ failures. In case of failure, new tasks are automatically created on available infrastructure.
Other components, such as VPCs, ALBs, and networking configurations, are designed to be fault-tolerant and ensure minimal downtime. Load balancing and auto-scaling mechanisms allow us to dynamically adjust capacity as needed.

Frontend components
Our frontend infrastructure is highly redundant and globally distributed, ensuring high availability and resilience against localized outages.

Storage
Our storage service provides highly redundant storage designed to provide **99.999999999% durability** and **99.99% availability** of objects over a given year. Additionally, we have versioning enabled for customer data. This ensures that any **accidental deletions or overwrites can be recovered**.

Extreme Disaster Scenarios
In an extreme scenario such as account compromise or ransomware attack, all our infrastructure can be recreated in a separate account and a region of our choice. This ensures minimal downtime and a secure restoration process in the worst-case scenario.

Compliance & Continuous Improvement

We align with industry best practices and regulatory requirements to maintain a secure environment for our Users. Our Information Security Management System is **ISO 27001:2022 certified**, and we are aligned with **GDPR**.

Our security policies are regularly reviewed and updated to address evolving threats, regulatory changes, and business needs. We conduct periodic risk assessments, internal audits, and employee training to strengthen our security posture and drive ongoing improvements.

Contact & Reporting Security Concerns

Users can report security concerns or vulnerabilities by contacting us at security@mentimeter.com. We encourage responsible disclosure and appreciate the efforts of security researchers in helping us maintain a secure platform.

Mentimeter also has a closed HackerOne Responsible Disclosure Program which researchers can refer to.

SECURITY AT MENTIMETER

Mentimeter