Security & Privacy at monday.com

monday.com

Answers to Frequently Asked Questions
Get the answers you need

Welcome to monday.com's security & privacy FAQ. In this document, you will find answers to important questions that we are frequently asked regarding the security of our application and infrastructure, as well as details regarding our API and incident readiness. While this document contains answers to our most frequently answered questions, should you have any additional questions or clarification requests, please contact our 24/7/365 support team at support@monday.com.

Table of contents

Corporate Security

1   **Q: Does monday.com have a formal information security program in place?**
A: Yes. The program takes into account local and international applicable laws, standards and regulations applicable to monday.com, and defines the measures and controls that we have in place designed to protect the monday.com service and its customers' data.
The program is based on ISO 27001 and includes in its scope the entire monday.com organization, including its subsidiaries, employees, contractors, subcontractors, partners and anyone who creates, maintains, stores, accesses, processes or transmits monday.com's or its users' information in connection with performance of the service provided by monday.com.

2 **Q: Which Security and Privacy related regulations, standards and certifications does monday.com comply with as of the date hereof?**

A: We have the following certifications, reports and compliance programs:

ISO 27001   ISO 27017   ISO 27018   ISO 27032

ISO 27701   SOC 1 Type II   SOC 2 Type II   SOC 3

HIPAA   GDPR   CCPA   aws partner network   CSA cloud security alliance®

You can find all of our certificates here.

3 **Q: Does monday.com have dedicated Security personnel?**

A: Yes. Our security efforts are guided and monitored by our Security Team and wider Security Forum, which is composed of representatives from Infrastructure, R&D, Operations and IT Teams.

4 **Q: Does monday.com have a formal process in place to address updates to privacy laws/regulations and regulatory guidance?**

A: Our Privacy Forum, which is composed of representatives from our Legal, Privacy and Security Teams and led by our DPO, continuously monitors updates to applicable privacy laws/regulations and regulatory guidance. The Forum is responsible for upholding our "Privacy by Design" approach, and regularly evaluates the implications that new or proposed product developments and other initiatives will carry in relation to data protection.

5 **Q: Is monday.com PCI-DSS compliant?**

A: monday.com uses the services of a PCI-DSS certified billing processor; thus, any credit card payments paid through our third party billing processor are PCI-DSS compliant. monday.com's service is not certified for PCI-DSS and

accordingly it does not process billing information on its service, thus PCI-DSS data is not stored on our service.

6 **Q: Does monday.com have an information security awareness program?**
A: Yes. As part of our initial onboarding process, as well as on an ongoing basis (at least annually), our employees receive training regarding their respective information security obligations.
Quarterly Security & Privacy Weeks are conducted to further elevate awareness amongst all company employees. In addition, developers undergo periodic security training in order to keep them up-to-date with security related development best practices on an annual basis, at minimum.

7 **Q: How frequently are monday.com's information security policies reviewed?**
A: Our information security policies are reviewed at least annually, or upon a material change to our service or security and privacy posture.

8 **Q: Does monday.com have a Privacy Notice/Policy?**
A: Yes, you can find our Privacy Policy here.

9 **Q: Does monday.com engage any processors/sub-processors who will have access to the personal data you share with us?**
A: Yes, we use a few sub-processors for the performance of our service. A list of our sub-processors (processing data on your ultimate behalf), including their location and the type of service they provide us with, is available here.

You can also subscribe to receive email notifications regarding any changes made to our sub-processors list through the link above.

Application Security

10 **Q: What type of data does monday.com collect?**

A: Upon creation of a new account, we store your personal data provided to us by you, such as: the user's full name, email address and phone number.

When you start using the monday.com service, the data stored by us will depend on your usage of the service and the type of data (such as text, files, etc.,) you and your authorized users who are signed into the service decide to submit and upload to monday.com.

Further information can be found in our [Private Policy](#).

11 **Q: How does monday.com secure its users' access into the monday.com service?**

A: Access into monday.com is performed via the following authentication methods:

- Credentials: username (usually your email address) and password;
- We also support the use of external identity providers, such as Google SSO (for Pro & Enterprise plan only) and Okta, OneLogin and custom SAML 2.0 (for Enterprise plan only);
- In addition, two-factor authentication (2FA) via a text message or through an authenticator app can be optionally enabled by the account administrators.

12 **Q: Does monday.com support the configuration of password policies?**

A: We provide administrators with a choice of two passwords strength settings for their account: 8 characters minimum with no repeating or consecutive characters allowed; or 8 characters minimum with no repeating or consecutive characters allowed and an inclusion of at least one digit (123), one lowercase letter (abc) and one uppercase letter (ABC).

13 **Q: Is monday.com customers' data encrypted? What methodologies are used to encrypt data?**
A: Yes, monday.com uses the following methods to encrypt customer data:

- Data at rest is encrypted using AES-256.
- Data in transit across open networks is encrypted using TLS 1.3 (at minimum TLS 1.2).
- User passwords are hashed and salted.

14 **Q: How does monday.com ensure that its code is being developed securely?**
A: We use OWASP Top 10 and CVSS standards to build in security for our software development lifecycle. All code written by our developers is statically analyzed and peer reviewed to ensure code quality before its deployment. We continuously evaluate and monitor our application for vulnerabilities during and after deployment.

15 **Q: Does monday.com perform application security testing?**
A: Yes, application penetration testing is performed on an annual basis by a varying independent third party. Additionally, we maintain a managed bug bounty program and DAST scans are performed at minimum on a biweekly basis.

16 **Q: How long does monday.com retain my data? What happens to it if I stop using the service?**
A: monday.com customers retain full control of their uploaded data and may modify or delete it at all times during their subscription term - using the means available to them through monday.com's user interface.
You can request deletion of your data as part of the account closure procedure, which is done through monday.com's admin panel. All your submitted data will then be deleted within 90 days, which includes a 30-day period to allow for rollback, and additional 60 days to delete the data from

our databases and our sub-processors' databases.

Alternatively, you may opt to keep your account's data even after you close your account and cancel your subscription, in which case our current policy is to retain it but without commitment to a specific duration. In such cases, we may delete it with or without notice.

Please note that you can export data from your account at any time in two formats:

- Boards can be exported to excel;
- The entire account's data can be exported through the administrator panel into a zip archive containing excel sheets and the files uploaded to the account (limited to administrators only).

17 Q: Does monday.com provide audit logs of user activity in the platform?
A: Yes, logs are provided in two forms:

- Board-level activity can be viewed in the Activity Log.
- Successful/failed login attempts can be viewed in the Audit Log.

18 Q: What authorization roles are available within the monday.com application?
A: Roles within our service include administrators, members, guests and viewers. You can find more details in the article here.
In addition, access control within our service is achieved by utilizing the following features: Workspaces, board types, board-level permissions, and column-level permissions.

19 Q: Does monday.com have an easily discoverable way for external parties to report security vulnerabilities?
A: Yes, security vulnerabilities can be reported to security@monday.com, or through our HackerOne vulnerability submission form here.

Infrastructure Security

20 **Q: Where are monday.com's data centers located?**
A: monday.com is a fully cloud-based service. Our service is hosted on Amazon Web Services infrastructure in Northern Virginia across multiple Availability Zones, with a DR site established in a different region. Certain backup data is stored on Google Cloud Platform (US, multi-region). These data centers employ leading physical and environmental security measures, resulting in highly resilient infrastructure. More information about their security practices is available at:
[AWS security page](#)
[GCP security page](#)

21 **Q: Is the monday.com service available in an on-premise version?**
A: monday.com is a fully cloud-based service and does not offer an on-premise version of its service.

22 **Q: How often is data backed up?**
A: We consistently backup user data every 5 minutes and distribute the encrypted backups across multiple AWS Availability Zones, where they are retained for 25 days. We have also established a disaster recovery site in a separate AWS region. Activity Log data is backed up to GCP (US, multi-region), where it is stored for 7 days.

23 **Q: Does monday.com have a Disaster Recovery Plan?**
A: Yes. Our DRP deals with disasters affecting our production environment and includes the restoration of the service's core functionality from our dedicated DR location. Testing is conducted at least twice a year.

24 **Q: Does monday.com have a physical security policy?**

A: Yes. Having said that, our service is fully cloud-based, with no part of our infrastructure retained on-premise. Physical security at our office includes access control based on personal identification, 24/7 CCTV monitoring and alarm systems.

25 **Q: How do you ensure your service's availability?**

A: We employ a microservices architecture to ensure minimal impact on system health in the case of failure of one or more components. Multiple Availability Zones are used to provide further redundancy and we have alternative providers for some of the services we rely on.

Enterprise customers are provided with a 99.9% SLA, subject to terms of the [SLA](#). Additionally, our service's availability can be monitored through our [status page](#), where you can also subscribe to receive updates via email or text messages.

26 **Q: Does monday.com employ best practices for secure architecture design?**

A: Yes, we are an [AWS Advanced Technology Partner](#). This serves as an attestation that AWS itself has rigorously vetted monday.com in terms of infrastructure, security, best-practice design and more.

27 **Q: Does monday.com support secure deletion of customer data?**

A: Yes. Our service is hosted on AWS, with certain data backed up to GCP. Both cloud computing providers implement proprietary data distribution and deletion strategies to allow for safe storage and deletion of sensitive data in a multi-tenant environment.

Storage media decommissioning is performed by the aforementioned providers using the techniques detailed in NIST 800-88.

Incident readiness

28 **Q: Does monday.com have a formal incident response plan?**

A: Yes. Our Incident Response Plan sets forth internal guidelines for detecting incidents, escalating them to the relevant personnel, communication (internal and external), investigation, mitigation and post-mortem analysis.
Further information can be found in Section 7 (Data Incident Management and Notification) to our DPA.

29 **Q: How will monday.com inform me if an incident or a breach have compromised my personal data?**

A: The format would depend on the type, scope and scale of the incident, though at minimum it will include an email sent to your account administrator(s). You would be informed to the extent available of the nature of the breach, the harmful effects of which monday.com is aware, and the actions monday.com has taken and plans to take.

Integration options

30 **Q: Does monday.com offer API access?**

A: Yes, you can find documentation on our GraphQL API here.

31 **Q: Does monday.com support further integrations with its service?**

A: Yes. In addition to our API, we support Integrations with various other software solutions to create customized workflows, including Zoom, Slack, Zendesk, Microsoft Teams, Salesforce, Outlook and more.
This is an optional capability which can be disabled through the admin panel.