Service Organization Control 3 (SOC 3)

For the Period April 1, 2022 to March 31, 2023

Report of monday.com Work Operating System

Relevant to Security, Availability, Confidentiality and Privacy

Kost Forer Gabbay & Kasierer
144 Menachem Begin St.
Tel-Aviv 6492102, Israel

Tel: +972-3-6232525
Fax: +972-3-5622555
ey.com

Report of Independent Accountants

To the Management of monday.com:

We have examined management's assertion that monday.com, during the period April 1, 2022 to March 31, 2023, maintained effective controls to provide reasonable assurance that:

- The System was protected against unauthorized access, use, or modification
- The System was available for operation and use, as committed or agreed
- Information within the System designated as confidential is protected as committed or agreed

Based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP Section 100 (2017), Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of monday.com's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included:

- (1) Obtaining an understanding of monday.com's relevant to security, availability, confidentiality and Privacy controls.
- (2) Testing and evaluating the operating effectiveness of the controls.
- (3) Performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, monday.com's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, confidentiality and Privacy.

Very truly yours,

Kost Forer Gabbay and Kasierer

Kost Forrer Gabbay & Kasierer
A member firm of Ernst & Young Global
May 8, 2023
Tel Aviv, Israel

Management Assertion on the controls over monday.com Work Operating System, based on the AICPA Trust Services Principles and Criteria for Security, Availability, Confidentiality and Privacy

We, as management of, monday.com Ltd. ("monday.com" or " the Company") are responsible for:

- Identifying the monday.com Work Operating System (system) and describing the boundaries of the system, as presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of our system, as presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the monday.com Work Operating System (system), to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved, based on the criteria relevant to security, availability, privacy and confidentiality set forth in the AICPA's TSP Section 100 2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016).

Yours sincerely,

Signature DocuSigned by:

9734413E9EF64B8...

Title

Description of the monday.com Work Operating System

Company Overview and Background

The company was founded in February 2012 and the product was launched as an independent startup in 2014. The company also became public in June 2021. monday.com is a SaaS Platform that transforms the way teams work together. An enterprise-grade platform where teams and organizations create the tools they need to run every aspect of their work, easily and efficiently. The Company's mission is to help teams build a culture of transparency, empowering everyone to achieve more and be happier at work.

Organizational structure

monday.com's organizational structure provides the overall framework for planning, directing and controlling operations for monday.com Work Operating System. It utilizes an approach whereby personnel and business functions are segregated according to job responsibilities. This approach allows the Company to clearly define responsibilities, lines of reporting and communications, and allows employees to focus on the specific business issues impacting their clients.

The Research and Development (R&D) department is responsible for designing and developing new features and capabilities of monday.com Work Operating System, according to functional requirements and specifications driven by client and market needs as determined by the Management Team, and in accordance with monday.com's internal security and privacy policies and guidelines.

The Consulting department's duties and responsibilities are:

- Servicing existing accounts, obtaining orders and introducing new accounts
- Adjusting content of sales presentations by studying the type of sales outlet
- Focusing sales efforts by studying existing and potential needs of clients
- Keeping management informed by submitting activity and results reports, such as daily call reports, weekly work plans, and monthly and annual territory analyses
- Recommending changes in products, service, and policy by evaluating results and competitive developments
- Resolving customer complaints by investigating problems; developing solutions; preparing reports; making recommendations to management

The CEOs are responsible for all company's operations and activities, and report on a quarterly basis to the Board. The CEOs conduct weekly meetings with the Management Team and review all company activities including security and compliance efforts.

The Chief Information Security Officer (CISO) is responsible for defining and building the company's security roadmap, prioritizing efforts based on the company's key assets, implementing and enforcing security processes and controls. Ongoing risk management processes are conducted, security controls are defined (operational, physical and logical) and third-party vulnerability penetration tests are managed. The CISO shall report to Senior Management with the key responsibility to ensure that all production risks, exposures, and vulnerabilities are identified, controlled and managed.

The Data Privacy Officer (DPO) is an outsourced worker from an external privacy consulting company, which is involved in processes to monitor that the privacy procedures are maintained throughout monday.com's operations. Ongoing risk management processes and Privacy Impact Analysis are conducted, Privacy by Design is implemented throughout the development lifecycle and privacy controls are defined (operational, physical and logical). The DPO is also the point of contact for monday.com's representative in the EU with regard to the European Supervision Authority as well as for customers for any privacy-related inquiries or complaints as the GDPR requires.

Components of the system providing the defined services

monday.com's Policies and Communication

Formal written policies for the principles and processes within the organization are developed and communicated so that personnel understand monday.com's objectives. Responsibility and accountability for developing and maintaining the policies are assigned to the monday.com relevant. The assigned policy owner updates the policy annually and the policy is reviewed and approved by the Management Team.

Significant components of these policies include, among others:

- Organizational structure
- Responsibility for information assets
- Information classification and sensitivity
- Access Control
- Security incident response
- Communication security
- Change management
- Physical security

A description of the monday.com Work Operating System and its boundaries is documented and communicated to monday.com employees and customers within the internal portal and the monday.com application. monday.com has implemented multiple communication channels to monitor that processes function as they were designed, and potential issues are identified and resolved in a timely manner. Various operations and synchronization meetings are generally conducted on a monthly basis or other timely basis in accordance with the operational needs. monday.com managers are responsible for communicating relevant corporate information and job-related data to their direct employees.

Availability, confidentiality and security-related obligations are communicated to monday.com's employees through the confidentiality and non-disclosure agreements while client obligations are communicated within their contracts. In addition, an incident management application is available to monday.com employees in order to report breaches of the system security, availability, and confidentiality. Customer issues are reported within a dedicated CRM application.

Security and Logical Access

Overview

monday.com's production environment is hosted in AWS data centers across multiple availability zones. The production environment includes multiple AWS cloud components such as EC2 instances, Elastic Load Balancers, Lambda functions, SQS, SNS resources and more. The company also uses multiple database technologies such as relational database systems (e.g. MySQL, PostgreSQL), NoSQL (e.g. DynamoDB and MongoDB), and in-memory databases. Databases are highly available with automatic failover in case of software/hardware failure.
monday.com production network encompasses numerous components, including segmented internal networks, security and monitoring tools and services responsible for redundancy and scaling. The production network is built on several tiers, where each type of server has its own segment and access rules. The AWS infrastructure consists of synchronization components which can be scaled up when needed. The network is monitored using NIDS. Administrative access to the AWS management interface is restricted to authorized personnel.

Logical Access

monday.com has established an information security policy designed to protect information at a level commensurate with its value (refer to the policy section above). The policy dictates security controls for media where information is stored, the systems that process it, as well as infrastructure components that facilitate its transmission. New users that

are granted access to the production environment and database are approved by monday.com's IT Team.

Production environment – AWS

As mentioned above, monday.com's production environment is hosted in AWS data centers across multiple availability zones.

User Permissions management

monday.com manages and delivers its services using AWS. Information security controls and procedures are implemented throughout these systems to help prevent unauthorized access to data. Access to system resources is protected through a combination of a DDoS Mitigation service, reverse proxies, firewalls, application controls and intrusion detection monitoring software. monday.com employees are provided with unique, personal user accounts that enable them to access the corporate cloud account. Access to monday.com's sensitive environments (production, AWS management interface, DDoS Mitigation platform, company's shared drive etc.) is performed using 2FA. Employees are provided with the minimal access rights required to carry out their duties. Access to the production environment, where information resources that are not deemed to be public reside, including the domain, databases and other production related environments, is granted upon approval by the IT Team. In addition, access to the database is restricted to authorized personnel only.

Usernames and passwords are used to authenticate personnel who need to access a system or a resource. Where applicable, strong password configuration settings are enforced through a directory service, including: (1) forced password change at defined intervals, (2) a minimum password length, (3) a limit on the number of attempts to enter a password before the user ID is suspended, and (4) password complexity. Due to system limitations, some configuration parameters may not be available on certain systems. Access to the internal production environment components is restricted to specific authorized IP addresses.

Recertification of Access Permissions

monday.com has implemented an access recertification process to help monitor that only authorized personnel have access to the systems, environments and databases. Permissions with the different production services in use by monday.com are reviewed and approved by monday.com's infrastructure team on a quarterly basis.

Access Revocation

User accounts are disabled or deleted on the production, application and database and the Company's assets are returned in a timely manner upon notification of job termination. Termination notifications indicating the employee's expected last day are sent to the relevant function: Management, HR, Finance, and IT. Terminated employees complete a termination clearance process on their last day at monday.com. This process includes revocation of access permissions to the systems and premises, as well as the return of the Company property, data and equipment.

Physical Access

monday.com recognizes the significance of physical security controls as a key component in its overall security program. Physical access methods, procedures and controls have been implemented to help prevent unauthorized access to data, assets and restricted areas. Physical access to monday.com's office is restricted to authorized personnel using fingerprint identification. Visitors to the monday.com office are accompanied while on premises.

Remote Access

monday.com networks are protected using commercial firewalls, which are configured and administered by the IT Team. monday.com employees are granted remote access to the production environment based on the need-to-know principle. In addition, remote site-to-site access to the production network is accomplished through a secure connection and its use is restricted to company's personnel only. monday.com's information security policy institutes the use of an antivirus solution, and employees who are granted remote access permission are required to protect their workstation from unauthorized users, and all employees' workstations are secured using antivirus software. Also, customer environments are segregated at the application and database level using unique IDs that are the result of a combination between several parameters. These are set when the customer registers to the application.

Vulnerability and penetration testing

monday.com's security program includes testing for security vulnerabilities by an independent security assessment service provider. A penetration test is performed on an annual basis. High-severity issues are investigated and taken care of as part of the SDLC process or by any necessary means. In addition, monday.com has a managed bug bounty program, through which security researchers from around the world are allowed to privately and responsibly disclose security vulnerabilities they have found, in exchange for a monetary reward. The penetration testing includes, among others, procedures to prevent customers, groups of individuals, or other entities from accessing confidential information other than their own. Input fields in the monday.com application are automatically sanitized in order to prevent code injection. In addition, automated vulnerability tests are performed to the application environment on a weekly basis in order to detect potential security vulnerabilities.

Security Awareness and Training

To help ensure that monday.com employees are aligned with the security practices and are aware of their duties, monday.com has implemented an internal security awareness program, including conducting a quiz in order to measure the effectiveness of this program. In addition, R&D department personnel go through dedicated security awareness training on a biannual basis.

Software Development Lifecycle ("SDLC") and Change Management

Software development at monday.com is performed in a controlled manner, to help ensure applications are properly designed, tested, approved and aligned to the monday.com business objectives. Personnel responsible for the design, development, implementation and operation of systems affecting Security, Availability and Confidentiality related issues have the qualifications and resources to fulfill their responsibilities. The R&D team conducts regular sessions and training in order to keep the teams up to date with the latest technologies and techniques, while creating awareness of the latest threats and methods to mitigate them. Changes are documented and prioritized using tasks within the change management application. Changes are tagged within the change management application in order to identify changes that impact security, availability and confidentiality. The permission to merge tested versions into Master branch is restricted to authorized personnel. Administrative access to the source control application is restricted to authorized personnel.

The code is verified manually in the local and staging environment. During the testing stage the code goes through 6 specific phases and includes tests:

1. Static code analysis
2. Unit test
3. End-to-end test: monday.com performs end-to-end testing in its test environment
4. Integration test
5. Automatic detection of potential security vulnerabilities in our dependencies
6. Code coverage monitoring which reports current levels and recent changes to coverage

A Continuous Integration (CI) tool is used to monitor testing phases. Pull requests are performed in order to deploy code changes. The pull requests include, among others: (1) Mandatory code review, (2) An automated security code review and (3) Testing. Code changes are reviewed along with the pull request performed by the developer. Code review by another developer is mandatory in order to continue the SDLC process and deploy a version to the production environment, and it is documented within the pull request itself. A dedicated tool is used in order to review the code coverage upon submitting a pull request. Thresholds are defined and implemented. Only after all preliminary checks have passed, the dedicated developers will deploy the code to the production environment.

Change Initiation

New feature developments are initiated by the Product Team while paying close attention to customer needs and requests. Technical improvements, bug fixes and security requirements are initiated also by clients and reviewed by the R&D Team. Feature flags are used in order to manage the feature deployment to customers. This capability enables rollback as well. Changes to the database environment needed to support application changes are performed according to defined procedures, reviewed by the database administrator, and tracked in a dedicated change management application that includes a history of changes and approvals. Additionally, significant changes performed to the application are communicated to monday.com's customers through the monday.com application. Changes performed to the production environment are followed by a notification to key monday.com personnel via internal communication tool.

Monitoring

Changes that may affect system security, availability or confidentiality are defined and communicated through the change management application. monday.com implements segregation of duties throughout its change management process. The production environment is restricted to authorized personnel on a need-to-know basis, enabling monday.com to minimize the possibility of unauthorized changes.

Infrastructure Change Management Overview

monday.com regularly makes changes within its production environment in response to change requests. These changes include routine maintenance activities, virtual machine and software updates, and other infrastructure-related changes. Change management procedures have been implemented by the Infrastructure Team to help manage and maintain the production environment in an orderly and controlled manner. The change management procedure supports the business objectives of monday.com's clients and ensures the availability, confidentiality, security and privacy of monday.com's services and data. monday.com uses a change management system to manage key tasks, such as the identification, prioritization, assignment, resolution and notification required by enterprise-critical functions. monday.com's change management processes incorporate the following key components:

- Approval of changes prior to implementation;
- Documentation of change requests, workflow and history in the ticketing system;
- Execution of major changes within a defined maintenance window in order to minimize potential risks to services and clients.

Support and Operations

monday.com's customer support procedures are designed to handle and resolve issues and requests in a timely manner. This includes issues that are internally identified, or issues submitted by clients. All customers are provided with 24/7/365 support via support mail, support hotline and customer support portal. Support is handled by monday.com according to its internal Service Level Agreement policy and procedure.

A help-desk department is available at monday.com. Issues raised to the help desk are documented within the CRM tool. Customer issues are addressed based on the internal SLA policy and procedures.

Additionally, reports of issues that require development work to be carried out for their resolution are escalated to the relevant R&D department personnel. Support meetings with the management are performed on a weekly basis,

in order to report major open issues to the management.

Escalation Process

Tickets escalation is done automatically through the system. monday.com's objective as it relates to escalation is to resolve issues during the first contact. If the first contact resolution is not possible, the issue is escalated to the next level of technical support. The escalation process is defined and documented in a matrix managed by Customer Support. A dedicated internal system is used to track and manage bugs. Decisions regarding the bug status are updated during bi-weekly iteration meetings with the R&D team leaders. Service interruptions are communicated to monday.com's customers according to the internal escalation procedure.

Emergency Procedures

An emergency change is a change deemed critical enough that it is implemented outside of the regular maintenance window and does not follow the routine approval process. In a case of an emergency change, authorized personnel make the change in order to maintain the level of service in the production environment. Emergency changes are documented, reviewed and. Changes performed to the production environment are followed by a notification to key monday.com personnel via an internal communication tool.

Availability procedures

Database backup and restoration

monday.com utilizes AWS backup services for the management and performance of backup tasks of various types of service- related data retained within the production environment, to enable availability and redundancy of data. Databases are redundant within the production environment. The monday.com application database is backed up according to the backup policy. The access to the backup and offline storage is restricted to authorized individuals. The monday.com databases are replicated to the cloud backup application.

Disaster Recovery Plan (DRP)

monday.com has developed a Disaster Recovery Plan to enable the company to continue to provide critical services in case of a disaster. The DRP is tested at minimum on an annual basis.
monday.com maintains a redundant infrastructure located at multiple locations within AWS environments. Those servers have been designed to provide clients with high availability services.

Confidentiality Procedures

Customer confidentiality is a key factor for monday.com. As such, monday.com has implemented security measures to ensure the confidentiality of its customers' sensitive personal information. The security measures aim to prevent unauthorized access, disclosure, alteration or destruction of sensitive personal information. Data at rest and backup files (database etc.) are encrypted. Cookies are either marked using the "HTTP" and "Secure" flags to prevent their unencrypted transmission, and/or cryptographically signed to prevent tampering. Encryption between monday.com's customers and the monday.com application is performed using an authenticated SSL tunnel. In the event that a disclosed confidentiality practice is discontinued or changed to be less restrictive, impacted customers are notified. Also, the infrastructure third party providers sign confidentiality agreements with monday.com in order to maintain the conformity of the system's confidentiality with monday.com's confidentiality policy. A confidentiality agreement is disclaimed as it relates to contracts with infrastructure third party providers in accordance with monday.com security policy.

Privacy Procedures

Management

Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring, and updating monday.com's privacy policies. The names of such a person or group and their responsibilities are defined. To help ensure that monday.com employees are aligned with security practices and are aware of their duties with regards to data privacy, monday.com has implemented a security and privacy awareness training detailing the secure handling of company confidential information, including customer data. The mandatory training is conducted for new and existing employees.

Notice

monday.com provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy. The monday.com privacy policy is available on its website and fully discloses the type of information the company may collect from the monday.com application and website, as well as how monday.com may use this information. The monday.com privacy policy is reviewed and updated by management on at least an annual basis.

As a responsible business, monday.com recognizes at senior levels the need to comply with the GDPR and to ensure that effective measures are in place to protect the personal data of its customers, employees and other stakeholders.

As part of meeting its legal obligations, an information security policy is available in both paper and electronic forms and is communicated within the organization and to all relevant stakeholders and interested third parties.

Commitment to the delivery of information security extends to senior levels of the organization, and is demonstrated through the information security policy and the provision of appropriate resources, in order to establish and develop effective information security controls.

Top management also ensures that a systematic review of performance of the program is conducted on a regular basis to ensure that information security objectives are being met and relevant issues are identified through the audit program and management processes.

A risk management approach is used which is in alignment with the requirements and recommendations of the GDPR and relevant international standards such as ISO/IEC 27001:2013.

Risk management takes place at several levels within the organization, including:

1. Assessment of risks to the achievement of information security objectives
2. Regular information security risk assessments within specific operational areas
3. Assessment of risk as part of the business change management process
4. At the project level as part of the management of significant change

****