Global Information Security Policy

MDY-ORG-POL-01

Code	MDY-ORG-POL-01
Version	2.4
Date of Version	Feb 2024

Table of Contents

1. Introduction

1.1. Purpose

The purpose of the Global Information Security Policy (GISP) is to define the measures and controls that monday.com has in place in order to protect its assets, data and customer data, and to comply with applicable local and international laws, standards and regulations.
It serves as a central policy document to which all monday.com employees must be aligned with, and defines actions and prohibitions that must be followed.

1.2. Scope

The scope of this policy is all monday.com's assets including, but not limited to customer data, monday.com's source code, diagrams, business information, PII and PHI (where applicable).

The scope of this policy is the entire monday.com organization, including its subsidiaries, employees, and applicable external workers, partners and anyone who creates, maintains, stores, accesses, processes or transmits monday.com data, as applicable.

1.3. Definitions

CEO: The Chief Executive Officer is responsible for the overall privacy and security practices of the company.

CISO: The Chief Information Security Officer is responsible for all information security aspects of the company.

DPO: The Data Protection Officer is responsible for ongoing privacy compliance and serves as a point of contact on privacy matters for data subjects and supervisory authorities and ensures compliance with data protection laws and regulations.

Confidentiality: The information is available or disclosed only to those authorized for it to unauthorized.

Integrity: All information assets are accurate and complete.

Availability: All information is accessible and usable upon demand.

Encryption: The process of transforming information using an algorithm to make it unreadable to anyone other than those who have a specific "need to know".

Personally identifiable information (PII): Any information about an individual that can be used to distinguish or trace an individual's identity, such as name, Identification number, date and place of birth, biometric records, medical information, financial information, etc.

Third Party: All vendors, external workers and other parties under contract with monday.com.

1.4. Information Security Objectives

- Align with monday.com business objectives and support the company's effort to achieve these objectives.
- Ensure that all security efforts are aligned with the company's obligations as a public company, and its fast growing pace.
- Maintain a comprehensive and up-to-date information security plan to mitigate applicable information security risks.
- Prevent security incidents at their earliest stage, and if they occur detect and contain security incidents as early as possible.

1.5. Organization of Information Security

monday.com's CISO has an overall responsibility for the company's information security. To provide guidance and continuous monitoring of the company's practices, the following representatives, at a minimum, shall conduct a security leadership sync on a monthly basis:

- CISO
- Application Security Team Lead

- Field CISO & Security Group Lead
- Information Security Team Lead
- GRC Team Lead
- Data Security Team Lead

Additional representatives from the company's departments may join the forum as needed.

1.6. Information Security Management

All monday.com's employees, and applicable third parties, must adhere to the company's policies, have their relevant responsibilities communicated to them as part of their onboarding and on a regular basis, and the applicable personnel should have 24/7 access to the relevant policies. All policies should be reviewed at least annually. Whenever there is a major change in the company's practices that may affect the confidentiality, integrity or availability of the company or its customers' data, the applicable policies will be reviewed and updated as needed. All policies must be approved by senior managers.

1.7. Continuous Improvement

monday.com continuously assesses potential risks to its operation and evaluates the need for protective measures, basing off its remediation strategy on the findings' severity.

The following periodic assessments are executed:

- Bug bounty program (application-level) - on an ongoing basis;
- Vulnerability scans (cloud & endpoints) - on an ongoing basis;
- Vendor assessment reviews - on an ongoing basis;
- Resilience status - monthly
- RedTeam drill - bi-annually

- Application-level PT - Annually
- ISO 27001, 27017, 27018, 27032, 27701 and SOC 1 Type II, SOC 2 Type II, SOC 3 audits - Annually

For more information regarding the Risk Management process, please refer to the **Risk Management Policy (MDY-ORG-POL-05**).

2. Roles and Responsibilities

Conflicting duties and areas of responsibilities should be segregated to reduce the opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

2.1. Senior Management

The senior management of the company has overall responsibility for ensuring that the company's commitment to this policy is met. The Senior Management should provide adequate resources to maintain and improve the Information Security Management System (ISMS) within the company.

2.2. CPTO

The CPTO (Chief Product & Technology Officer) has overall responsibility for ensuring that the company's commitment to this policy is met. The CPTO should provide adequate resources to maintain and improve the Information Security Management System (ISMS) within the company.

2.3. CISO

The CISO is responsible for defining the company's security strategy, implementing information security processes and controls and their enforcement. The CISO reports to the CPTO. The CISO's main responsibilities are:

- Ownership of the Information Security Management System (ISMS) documentation.
- Leading the process of periodic risk assessment as part of the security policy and sharing it on a quarterly with monday.com's senior management.
- When applicable, recommend changes to the policies, standards and procedures.
- Ensuring that all critical company assets are secured and controlled.
- Developing and maintaining an information security education, training and awareness program.
- Advising on compliance with laws, regulations, best practices and frameworks.
- Building security-related budget and plans.

2.4. DPO

The DPO (Data Protection Officer) is responsible for:

- Monitoring and advising on the ongoing privacy compliance.
- Serving as a point of contact on privacy matters for data subjects and supervisory authorities.
- Review in collaboration with the Legal Department the relevant sections in the Personal Information Management System (PIMS) documentation.
- When applicable, recommend changes to the policies, standards and procedures as they relate to data protection.
- Advising on compliance with data protection laws, regulations, best practices and frameworks.

2.5. Security Audit Committee

The security steering committee is responsible for reviewing the security strategic planning and approving it. The security steering committee will meet on a quarterly. The security steering committee members are:

Relevant board members:

- CEO/s
- CPTO
- CFO
- General Counsel
- CISO

2.6. Asset Owners

Asset owners are employees held accountable for the protection of significant assets. Asset owners are responsible, as applicable, for:

- Appropriate classification of information assets.
- Specifying and funding suitable protective controls.
- Authorizing access to information assets in accordance with classification and business needs.
- Ensure timely completion of regular reviews.
- Monitoring compliance with protection requirements affecting their assets.

2.7. Employees

All employees are required to comply with the company's information security policies and standards and must use company assets according to the **Acceptable Use Policy (MDY-ORG-POL-02)**.

3. Information Security Implementation

3.1. Human Resources

A company's employees are one of the most valuable resources it has. Employees have access to sensitive information by virtue of their job. Securely managing the human resources of monday.com is an essential part of the overall security of the company and is covered in the **HR Security Policy** (**MDY-HR-POL-01**).

3.2. Asset Management

Lack of knowledge and familiarity with the targets of attacks in an organization poses a significant risk. Mapping an organization's assets and defining the measures to secure them significantly decreases the risk level of an organization.

- All relevant Company assets (such as data, software, hardware, etc.) will be accounted for and have an owner.
- Asset Owners will be identified for all relevant assets, and will be responsible for the maintenance and protection of their assets.
- All information should be classified and handled according to its sensitivity levels as detailed in the **Data Classification Policy** (**MDY-ORG-POL-04**).
- Asset management security is detailed in the **Asset Management Policy** (**MDY-IT-POL-02**).

3.3. Access Control

Accessing assets is one of the most sensitive processes in an organization. Failure to uphold appropriate access privileges to resources may put the organization at a significant risk. Access privileges at monday.com are provided according to the need-to-know and least privilege principles. All security aspects of access control are detailed in the **Access Control Policy** (**MDY-IT-POL-01**).

3.4. Cryptography

monday.com manages sensitive information on behalf of its customers, in addition to information pertaining to its internal operations. Encryption of such data both in transit (while being sent from one component to another), and at rest (when stored) is of crucial importance. monday.com's cryptographic security controls are detailed in the **Cryptographic Usage Policy** (**MDY-DEV-POL-04**).

3.5. Physical and Environmental Security

The physical and environmental security aspect refers to the measures that monday.com utilizes to secure its physical premises and assets. It is detailed in the **Physical Security Policy (MDY-PHY-POL-01)**.

3.6. Operations Security

The capacity management of the existing systems, and the process for accepting new updates within company systems, should be conducted according to the company policies. A change management process is in place to ensure that changes are well controlled. For more information, please refer to the company's **IT Change Management Procedure (MDY-IT-PRD-01)**.

To ensure the protection of the information monday.com handles on behalf of its customers against loss, backups shall be taken and tested regularly in accordance with the **Backup Policy** (**MDY-DEV-POL-03**). In addition, monitoring of monday.com's inbound and outbound data traffic will be in place, as detailed in **Data Loss Prevention (DLP) Policy (MDY-IT-POL-03)**.

3.7. Communications Security

Communications security deals with the prevention of unauthorized access to data in transit. Communication security is covered both in the **Physical Security Policy (MDY-PHY-POL-01)** and **Cryptographic Usage Policy (MDY-DEV-POL-04)**.

3.8. Supply Chain Security

monday.com uses third party solutions for certain aspects of its service. Third party relations may include cloud service providers, outsourced contractors, remote support, etc. When implementing a third party solution, certain security measures should be taken in order to ensure that the third party does not negatively impact monday.com's risk level. Supply chain security is covered in the **Third Party Security Policy** (**MDY-ORG-POL-07**).

3.9. Information Security Incident Management, Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

monday.com invests substantial efforts to prevent any incidents that may impact the confidentiality, availability and integrity of the data it processes on behalf of its customers. Notwithstanding this, it is not possible to fully mitigate the risk of incidents. In case of an information security incident, monday.com will detect and contain the incident in the shortest possible time frame. All aspects of information security incidents handling are covered in the **Information Security & Data Incident Response Procedure** (**MDY-ORG-POL-06**), **Business Continuity Plan (MDY-BCP-PLN-01)** and **Disaster Recovery Plan (DRP) (MDY-BCP-PLN-02)**

3.10. Product Security & Secure Development

monday.com's service processes sensitive and critical data on behalf of monday.com customers. The service should therefore be developed to the highest standards of security, to ensure the information's confidentiality, availability and integrity. To learn more about monady.com's secure development practices and vulnerabilities management, please refer to the **S-SDLC Policy** (**MDY-DEV-POL-01**) and the **Patch Management Policy** (**MDY-DEV-POL-02**).

3.11. Compliance

monday.com is committed to adhering to any applicable laws, regulations and standards. This is done by continuously identifying new local and international laws, new regulations and the publication of new standards. For more information please refer to **ISMS & PIMS Manual (MDY-ORG-POL-03)**.

4. Policy Lifecycle

4.1. Additions, Changes and Deletions

- Alterations to policies, standards and baselines should be made as necessary.
- Each request shall include a business justification for requesting such a change.
- The relevant senior manager shall review each request and provide approval / denial.
- The Security Team is responsible for ensuring all relevant changes or additions are communicated to the company's employees.

4.2. Review Process

- This GISP shall be reviewed and updated annually or when necessary, in accordance with business or regulatory requirements.
- Information security policies, standards and baselines shall be reviewed at least annually to ensure that they are consistent and properly address the following:
    - Business needs and business environment – controls should remain effective from both cost and ongoing operational perspectives, and support the business without causing unreasonable disruption to its processes.
    - External technology environment – opportunities and threats created by changes, trends, and new developments.
    - Internal technology environment – strengths and weaknesses resulting from the company's use of technology.
    - Legal, regulatory and contractual requirements.
    - Other requirements specific to new or unique circumstances.

4.3. Delegation of Responsibilities

- The CISO may choose to delegate certain roles and responsibilities to specific employees or units as required.
- Delegated responsibilities are non-transferable.

4.4. Exception to Policies

- The Company's employees and applicable third parties are required to comply with the said policies and standards.
- In the event that a policy or standard cannot be adhered to, an exception to such a baseline should be considered by the CISO.
- Exceptions should be assigned due-dates where applicable, to ensure the timely implementation of the agreed upon remediation strategies.
- Exceptions should be regularly reviewed to verify that remediation is achieved in time.