Global Information Security Policy

MDY-ORG-POL-01

Code	MDY-ORG-POL-01
Version	2.1
Date of Version	December 2020
Confidentiality Level	Public

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 information and its customers' information, and to comply with local and international laws, standards and regulations.

It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow.

1.2. Scope

The scope of this policy is all monday.com's information including customer information, source code, diagrams, financial information, PII and PHI (where applicable).

The scope of this policy is 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 information.

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 ensuring proper protective measures of personal data are in place, and overseeing the privacy aspect of the company's product and practices.

Confidentiality: The property that information is not made available or disclosed to unauthorized.

Integrity: The property of safeguarding the accuracy and completeness of assets.

Availability: The property of being 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, subcontractors and other parties under contract with monday.com.

1.4. Information security objectives

- Align with monday.com's business objectives and support the company's effort to achieve these objectives;
- Maintain a comprehensive and up-to-date information security plan to mitigate information security risks;
- Prevent security incidents at their earliest stage, and if they occur detect and contain security incidents as early as possible;
- Maintain an up-to-date list of all assets and the risks associated with these assets.

1.5. Organization of Information Security

monday.com's CISO has 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, conduct a Security Forum on a weekly basis:

- CISO
- VP Operations
- R&D Information Security Lead
- Head of Infrastructure
- Infrastructure Security Lead
- IT Manager
- Compliance Specialist

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

1.6. Information Security Management

All monday.com's employees, contractors and third parties should adhere to the company's policies, have their relevant responsibilities communicated to them as part of their onboarding and on a regular basis, and have 24/7 access to the 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's or its customers' data, the applicable policies will be reviewed.

All policies must be approved by a member of the senior management.

1.7. Continuous Improvement

monday.com continuously assesses potential risks to its service 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 - On an ongoing basis
- Application vulnerability scans - On an ongoing basis
- An overall risk assessment of the critical information systems - Annually
- Application level PT - 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. VP Operations

The VP Operations is responsible for approving security budgets.

In addition, the VP Operations communicates the results of essential ISMS activities (such as Risk Assessment, Risk Treatment Plan, Operational Plan and Goals, etc.) to both third parties (as applicable) and to Senior Management.

2.3. CISO

The CISO is responsible for defining the company's security strategy, implementation of information security processes and controls and their enforcement. The CISO reports to Senior Management.

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.
- 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 investment plans.

2.4. Security Steering Committee

The security steering committee is responsible for reviewing the security strategic planning and approving it. The security steering committee will meet once a year.

The security steering committee members are:

- CEO
- CTO
- VP Operations
- VP R&D
- General Counsel
- CISO

2.5. Information Security Forum

The Security Forum is the operational forum for all Information Security activities.

Its responsibilities are:

- Coordinating the development and implementation of information management practices including policies, standards, guidelines and procedures;
- Coordinating the development and implementation of security related issues in the company products, code and infrastructure;
- Addressing ongoing security related issues, raised by the company employees, vendors, partners, and customers;
- Coordinating and sharing information among Forum members to ensure consistent execution of the information security management activities across the organization.

The company's Security Forum will meet at least once a month.

2.6. Asset Owner

Asset Owners are managers held accountable for the protection of particular significant assets. They may delegate information security tasks to other individuals but remain accountable for proper implementation of the tasks. The Information Asset Owners are responsible for:

- Appropriate classification and protection of the information assets;
- Specifying and funding suitable protective controls;
- Authorizing access to information assets in accordance with the classification and business needs;
- Ensuring timely completion of regular system/data access 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 should use company assets according to the **Acceptable Use Policy (**MDY-ORG-POL-02**)**.

3. Information Security Implementation

3.1. Human Resources Security

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 Security

Lack of knowledge and familiarity with the targets of attack 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 Company assets (such as data, software, hardware, etc.) will be accounted for and have an owner;
- Asset Owners will be identified for all 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 in 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-IT-POL-04**).

3.5. Physical and Environmental Security

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

3.6. Operations Security

The capacity management of the existing systems, and the process for accepting new systems within the company, 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 an agreed policy, as detailed in the **Backup Policy** (**MDY-IT-POL-05**).

3.7. Communications Security

Communications security deals with the prevention of unauthorized access to information in transit - information that is sent from one IT entity to another one.

Communication security is covered both in the **Physical and Environmental Security Policy** (**MDY-PHY-POL-01**) and **Cryptographic Usage Policy** (**MDY-IT-POL-04**).

3.8. Supply Chain Security

monday.com uses third party solutions for certain aspects of its service. Such 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-IT-POL-06**).

3.9. Information Security Incident Management, Business Continuity Plan (BCP) and 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** (**DOC-15**), **Disaster Recovery Plan (DRP)** (**MDY-ORG-POL-03**) and **Business Continuity Plan (BCP)** (**MDY-BCP-PLN-01**).

3.10. Product Security and 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, in order to ensure the information's confidentiality, availability and integrity. To learn more about monady.com' secure development practice and vulnerabilities management, please refer to the **S-SDLC Policy** (**MDY-DEV-POL-01**) and to the **Patch Management Policy** (**MDY-DEV-POL-02**).

3.11. Compliance

monday.com is committed to adhere 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.

4. Policy Lifecycle

4.1. Additions, Changes and Deletions

- Alterations to established policies, standards and baselines should be made as necessary.
- Each request should include the business justification for requesting such a change.
- The VP Operations should 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

- The Global Information Security Policy should be reviewed and updated annually or when necessary, in accordance with business or regulatory requirements.
- Information security policies, standards and baselines should be reviewed at least every 12 months 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 third parties are required to comply with 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.
- An exception may be granted only if the benefits of the exception outweigh the resulting risks, as determined by the CISO based on the recommendation of the Security Forum.
- 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.