Globale Informationssicherheitsrichtlinie

MDY-ORG-POL-01

Code	MDY-ORG-POL-01
Version	2.2
Datum der Version	Nov. 2021
Erstellt/Aktualisiert von	Nitsan Tahal Bartov
Genehmigt von	Ouriel Weisz
Vertraulichkeitsstufe	Öffentlich

Änderungshistorie:

Datum	Version	Erstellt von	Genehmigt von	Beschreibung der Änderung
Nov. 2017	1.0	Yaniv Milhovitch	Ouriel Weisz	Erste Version
Juni 2018	1.1	Ouriel Weisz	Ouriel Weisz	Revisionen, Zusammenfassung hinzugefügt
Jan. 2019	1.2	Alex Barkin	Ouriel Weisz	Regelmäßige Überprüfung und Revision
Dez. 2019	2.0	Yuval Yelin	Shiran Nawi	Änderung des Inhalts. ISMS-konform
Dez. 2020	2.1	Mor Bouganim-Fogel	Ouriel Weisz	Regelmäßige Überprüfung und Revisionen
Nov. 2021	2.2	Nitsan Tahal Bartov	Ouriel Weisz	Regelmäßige Überprüfung und Revisionen

Inhaltsverzeichnis

1. Einleitung

1.1. Zweck

Der Zweck der globalen Informationssicherheitsrichtlinie (Global Information Security Policy – GISP) besteht darin, die Maßnahmen und Kontrollen zu definieren, die monday.com zum Schutz seiner Informationen und der Informationen seiner Kunden einsetzt und um die lokalen und internationalen Gesetze, Standards und Vorschriften einzuhalten.
Sie dient als zentrales Richtliniendokument, an dem alle Mitarbeiter und Auftragnehmer ausgerichtet sein müssen, und definiert Handlungen und Verbote, die alle Benutzer befolgen müssen.

1.2. Geltungsbereich

Der Geltungsbereich dieser Richtlinie umfasst alle Informationen von monday.com, einschließlich gegebenenfalls Kundeninformationen, Quellcode, Diagramme, Finanzinformationen, PII und PHI.

Der Geltungsbereich dieser Richtlinie erstreckt sich auf die gesamte monday.com-Organisation, einschließlich ihrer Tochtergesellschaften, Mitarbeiter, Auftragnehmer, Unterauftragnehmer, Partner und aller Personen, die Informationen von monday.com erstellen, pflegen, speichern, darauf zugreifen, sie verarbeiten oder übertragen.

1.3. Definitionen

CEO: Der Chief Executive Officer ist für die gesamten Datenschutz- und Sicherheitspraktiken des Unternehmens verantwortlich.

CISO: Der Chief Information Security Officer ist für alle Aspekte der Informationssicherheit des Unternehmens verantwortlich.

DSB: Der Datenschutzbeauftragte ist für die Gewährleistung angemessener Schutzmaßnahmen für personenbezogene Daten und die Überwachung der Datenschutzaspekte der Produkte und Praktiken des Unternehmens verantwortlich.

Vertraulichkeit: Die Informationen stehen nur denjenigen zur Verfügung, die dazu berechtigt sind.

Integrität: Alle Informationsbestände sind korrekt und vollständig.

Verfügbarkeit: Alle Informationen sind bei Bedarf zugänglich und verwendbar.

Verschlüsselung: Der Prozess, bei dem Informationen mit Hilfe eines Algorithmus so umgewandelt werden, dass sie für andere Personen als diejenigen, die sie „unbedingt kennen müssen“, nicht lesbar sind.

Persönlich identifizierbare Informationen (PII): Alle Informationen über eine Person, die zur Unterscheidung oder Rückverfolgung der Identität einer Person verwendet werden können, wie z. B. Name, Identifikationsnummer, Geburtsdatum und -ort, biometrische Daten, medizinische Daten, Finanzdaten etc.

Dritte: Alle Anbieter, Unterauftragnehmer und andere Parteien, die mit monday.com unter Vertrag stehen.

1.4. Ziele der Informationssicherheit

- Ausrichtung an den Geschäftszielen von monday.com und Unterstützung der Bemühungen des Unternehmens, diese Ziele zu erreichen.
- Sicherstellung, dass alle Sicherheitsmaßnahmen mit den Verpflichtungen des Unternehmens als öffentliches Unternehmen und seinem schnellen Wachstum in Einklang stehen.
- Aufrechterhaltung eines umfassenden und aktuellen Informationssicherheitsplans zur Minderung von Informationssicherheitsrisiken.

- Verhütung von Sicherheitsvorfällen im frühestmöglichen Stadium und, falls sie auftreten, möglichst frühzeitige Erkennung und Eindämmung von Sicherheitsvorfällen.
- Führung einer aktuellen Liste aller Vermögenswerte und der mit diesen Vermögenswerten verbundenen Risiken.

1.5. Organisation der Informationssicherheit

Der CISO von monday.com hat die Gesamtverantwortung für die Informationssicherheit des Unternehmens.

Um die Praktiken des Unternehmens zu lenken und kontinuierlich zu überwachen, führen die folgenden Vertreter mindestens einmal pro Woche ein Sicherheitsforum durch:

- CISO
- VP Operations
- Leiter des Bereichs F&E-Informationssicherheit
- Leiter des Bereichs Infrastruktur
- Leiter der Infrastruktursicherheit
- IT-Leiter
- Compliance-Spezialist

Weitere Vertreter aus den Abteilungen des Unternehmens können dem Forum bei Bedarf beitreten.

1.6. Management der Informationssicherheit

Alle Mitarbeiter, Auftragnehmer und Dritte von monday.com müssen sich an die Unternehmensrichtlinien halten, ihre jeweiligen Verantwortlichkeiten müssen ihnen im Rahmen ihrer Einarbeitung und auf regelmäßiger Basis mitgeteilt werden und sie müssen rund um die Uhr Zugang zu den Richtlinien haben. Alle Richtlinien müssen mindestens einmal jährlich überprüft werden. Bei jeder größeren Änderung der Unternehmenspraktiken, die sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten des Unternehmens oder seiner Kunden auswirken kann, sind die geltenden Richtlinien zu überprüfen.

Alle Richtlinien müssen von einem Mitglied der Geschäftsleitung genehmigt werden.

1.7. Kontinuierliche Verbesserung

monday.com bewertet fortlaufend potenzielle Risiken für seinen Service und evaluiert die Notwendigkeit von Schutzmaßnahmen. Die Strategie zur Behebung von Problemen basiert auf der Schwere der festgestellten Mängel.

Die folgenden periodischen Bewertungen werden durchgeführt:

- Bug-Bounty Programm – auf fortlaufender Basis
- Scans der Schwachstellen von Anwendungen – auf fortlaufender Basis
- Eine allgemeine Risikobewertung der kritischen Informationssysteme – jährlich
- PT auf Anwendungsebene – jährlich
- Weitere Informationen über den Risikomanagementprozess finden Sie in der **Risikomanagementrichtlinie (MDY-ORG-POL-05)**.

2. Rollen und Zuständigkeiten

Widersprüchliche Aufgaben und Verantwortungsbereiche sind zu trennen, um die Möglichkeiten einer unbefugten oder unbeabsichtigten Änderung oder eines Missbrauchs der Vermögenswerte der Organisation zu verringern.

2.1. Geschäftsleitung

Die Geschäftsleitung des Unternehmens trägt die Gesamtverantwortung dafür, dass die Verpflichtung des Unternehmens zu dieser Richtlinie eingehalten wird.

Die Geschäftsleitung muss angemessene Ressourcen für die Aufrechterhaltung und Verbesserung des Informationssicherheitsmanagementsystems (ISMS) im Unternehmen bereitstellen.

2.2. VP Operations

Der VP Operations ist für die Genehmigung von Sicherheitsbudgets verantwortlich.

Darüber hinaus kommuniziert der VP Operations die Ergebnisse wesentlicher ISMS-Aktivitäten (wie z. B. Risikobewertung, Risikobehandlungsplan, Betriebsplan und -ziele etc.) sowohl an Dritte (soweit zutreffend) als auch an die Geschäftsleitung.

2.3. CISO

Der CISO ist für die Definition der Sicherheitsstrategie des Unternehmens, die Implementierung von Informationssicherheitsprozessen und -kontrollen sowie deren Durchsetzung verantwortlich. Der CISO ist der Geschäftsleitung unterstellt.

Die Hauptpflichten des CISO sind:

- Verantwortung für die Dokumentation des Informationssicherheitsmanagementsystems (ISMS).

- Leitung des Prozesses der regelmäßigen Risikobewertung als Teil der Sicherheitsrichtlinie.
- Gegebenenfalls Empfehlung von Änderungen an den Richtlinien, Standards und Verfahren.
- Sicherstellung, dass alle kritischen Vermögenswerte des Unternehmens gesichert und kontrolliert werden.
- Entwicklung und Aufrechterhaltung eines Ausbildungs-, Schulungs- und Aufklärungsprogramms zur Informationssicherheit.
- Beratung hinsichtlich der Einhaltung von Gesetzen, Vorschriften, bewährten Verfahren und Rahmenwerken.
- Erstellung von sicherheitsbezogenen Haushalts- und Investitionsplänen.

2.4. Lenkungsgruppe Sicherheit

Der Sicherheitslenkungsausschuss ist für die Überprüfung der strategischen Sicherheitsplanung und deren Genehmigung zuständig. Der Sicherheitslenkungsausschuss trifft sich einmal im Jahr.

Die Mitglieder des Sicherheitslenkungsausschusses sind:

- CEO
- CTO
- VP Operations
- VP F&E
- Rechtsberater
- CISO

2.5. Informationssicherheitsforum

Das Sicherheitsforum ist das operative Forum für alle Aktivitäten im Bereich der Informationssicherheit.

Seine Aufgaben sind folgende:

- Koordinierung der Entwicklung und Implementierung von Praktiken des Informationsmanagements einschließlich Strategien, Standards, Richtlinien und Verfahren;
- Koordinierung der Entwicklung und Implementierung von sicherheitsrelevanten Aspekten in den Produkten, dem Code und der Infrastruktur des Unternehmens;
- Adressierung laufender sicherheitsrelevanter Fragen, die von den Mitarbeitern des Unternehmens, Anbietern, Partnern und Kunden aufgeworfen werden;
- Koordinierung und Austausch von Informationen zwischen den Forumsmitgliedern, um eine einheitliche Durchführung der Aktivitäten im Bereich des Informationssicherheitsmanagements im gesamten Unternehmen zu gewährleisten.

Das Sicherheitsforum des Unternehmens trifft sich mindestens einmal im Monat.

2.6. Asseteigentümer

Asseteigentümer sind Manager, die für den Schutz bestimmter wichtiger Vermögenswerte verantwortlich sind. Sie können Aufgaben der Informationssicherheit an andere Personen delegieren, bleiben aber für die ordnungsgemäße Durchführung der Aufgaben verantwortlich. Die Eigentümer von Informationsbeständen sind verantwortlich für:

- Angemessene Klassifizierung und Schutz der Informationsbestände;
- die Spezifizierung und Finanzierung geeigneter Schutzmaßnahmen;
- die Genehmigung des Zugriffs auf Informationsbestände in Übereinstimmung mit der Klassifizierung und den Geschäftsanforderungen;

- Sicherstellung des rechtzeitigen Abschlusses von regelmäßigen System-/Datenzugriffsüberprüfungen;
- Überwachung der Einhaltung der Schutzanforderungen, die ihre Assets betreffen.

2.7. Mitarbeiter

Alle Mitarbeiter sind verpflichtet, die Informationssicherheitsrichtlinien und -standards des Unternehmens einzuhalten und die Unternehmensressourcen gemäß der **Richtlinie zur akzeptablen Nutzung (MDY-ORG-POL-02)** zu verwenden.

3. Implementierung der Informationssicherheit

3.1. Sicherheit im Personalwesen

Die Mitarbeiter eines Unternehmens sind eine der wertvollsten Ressourcen, die es besitzt. Die Mitarbeiter haben aufgrund ihrer Tätigkeit Zugang zu sensiblen Informationen. Die sichere Verwaltung der Humanressourcen von monday.com ist ein wesentlicher Bestandteil der Gesamtsicherheit des Unternehmens und wird in der **HR -Sicherheitsrichtlinie (MDY-HR-POL-01)** behandelt.

3.2. Asset-Management-Sicherheit

Mangelndes Wissen und mangelnde Vertrautheit mit den Angriffszielen in einer Organisation stellen ein großes Risiko dar. Die Erfassung der Assets eines Unternehmens und die Festlegung von Maßnahmen zu deren Sicherung verringern das Risikoniveau eines Unternehmens erheblich.

- Alle Assets des Unternehmens (wie Daten, Software, Hardware etc.) werden erfasst und haben einen Eigentümer;

- Für alle Assets werden Asseteigentümer identifiziert, die für die Wartung und den Schutz ihrer Assets verantwortlich sind;
- Alle Informationen müssen entsprechend ihrer Sensibilitätsstufe klassifiziert und behandelt werden, wie in der **Datenklassifizierungsrichtlinie (MDY-ORG-POL-04)** beschrieben.
- Die Sicherheit des Asset Managements wird in der **Asset-Management-Richtlinie (MDY-IT-POL-02)**. beschrieben

3.3. Zugangskontrolle

Der Zugriff auf Assets ist einer der sensibelsten Prozesse in einer Organisation. Werden keine angemessenen Zugriffsrechte auf Ressourcen aufrechterhalten, kann dies ein erhebliches Risiko für die Organisation darstellen.

Die Zugriffsrechte werden bei monday.com nach dem Need-to-know-Prinzip und dem Prinzip der geringsten Privilegien vergeben. Alle Sicherheitsaspekte der Zugriffskontrolle sind in der **Zugriffskontrollrichtlinie (MDY-IT-POL-01)** beschrieben.

3.4. Kryptographie

monday.com verwaltet zusätzlich zu den Informationen, die den internen Betrieb betreffen, sensible Daten im Namen seiner Kunden. Die Verschlüsselung solcher Daten ist sowohl bei der Übertragung (während sie von einer Komponente zur anderen gesendet werden) als auch im Ruhezustand (wenn sie gespeichert werden) von entscheidender Bedeutung. Die kryptografischen Sicherheitskontrollen von monday.com sind in der **Kryptographie-Nutzungsrichtlinie (MDY-IT-POL-04)** beschrieben.

3.5. Physische und Umweltsicherheit

Der Aspekt der physischen und Umweltsicherheit bezieht sich auf die Maßnahmen, die monday.com zur Sicherung seiner physischen Räumlichkeiten und Vermögenswerte einsetzt. Er wird in der **Richtlinie zur physischen und Umweltsicherheit (MDY-PHY-POL-01)** näher erläutert.

3.6. Betriebliche Sicherheit

Das Kapazitätsmanagement der bestehenden Systeme und das Verfahren für die Aufnahme neuer Systeme in das Unternehmen sind entsprechend den Unternehmensrichtlinien durchzuführen. Es gibt ein Änderungsmanagementverfahren, um sicherzustellen, dass Änderungen gut kontrolliert werden. Weitere Informationen finden Sie im **IT-Änderungsmanagementverfahren (MDY-IT-PRD-01)** des Unternehmens.

Um die Informationen, die monday.com im Namen seiner Kunden verwaltet, vor Verlust zu schützen, werden gemäß einer vereinbarten Richtlinie regelmäßig Backups erstellt und getestet, wie in der **Backup -Richtlinie(MDY-IT-POL-05)** beschrieben.

3.7. Kommunikationssicherheit

Die Kommunikationssicherheit befasst sich mit der Verhinderung des unbefugten Zugriffs auf Informationen im Transit – Informationen, die von einer IT-Einheit an eine andere gesendet werden.

Die Kommunikationssicherheit wird sowohl in der **Richtlinie für physische und Umweltsicherheit (MDY-PHY-POL-01)** als auch in der **Richtlinie für die Nutzung von Kryptographie (MDY-IT-POL-04)** behandelt.

3.8. Sicherheit der Lieferkette

monday.com nutzt Lösungen von Drittanbietern für bestimmte Aspekte seiner Dienstleistung. Solche Beziehungen zu Dritten können Cloud-Service-Provider, ausgelagerte Auftragnehmer, Remote-Support etc. umfassen. Bei der Implementierung einer Drittanbieterlösung müssen bestimmte Sicherheitsmaßnahmen ergriffen werden, um sicherzustellen, dass der Drittanbieter keine negativen Auswirkungen auf das Risikoniveau von monday.com hat.

Die Sicherheit der Lieferkette wird in der **Sicherheitsrichtlinie für Drittanbieter (MDY-IT-POL-06)** behandelt.

3.9. Management von Informationssicherheitsvorfällen, Business Continuity Plan (BCP) und Disaster Recovery Plan (DRP)

monday.com unternimmt erhebliche Anstrengungen, um Vorfälle zu verhindern, die sich auf die Vertraulichkeit, Verfügbarkeit und Integrität der Daten, die monday.com im Auftrag seiner Kunden verarbeitet, auswirken könnten. Ungeachtet dessen ist es nicht möglich, das Risiko von Vorfällen vollständig zu vermeiden. Im Falle eines Informationssicherheitsvorfalls wird monday.com den Vorfall in der kürzest möglichen Zeit aufdecken und eindämmen. Alle Aspekte der Behandlung von Informationssicherheitsvorfällen sind im **Verfahren für Informationssicherheit und Reaktion auf Datenvorfälle(DOC-15)**, **Disaster Recovery Plan (DRP) (MDY-ORG-POL-03)** und **Business Continuity Plan (BCP) (MDY-BCP-PLN-01)** geregelt.

3.10. Produktsicherheit und sichere Entwicklung

Die Dienstleistung von monday.com verarbeitet sensible und kritische Daten im Auftrag der Kunden von monday.com. Die Dienstleistung ist daher nach den höchsten Sicherheitsstandards zu entwickeln, um die Vertraulichkeit, Verfügbarkeit und Integrität der Daten zu gewährleisten. Um mehr über die Praxis der sicheren Entwicklung und das Schwachstellenmanagement von monday.com zu erfahren, lesen sie bitte die **S-SDLC-Richtlinie (MDY-DEV-POL-01)** und die **Patch-Management-Richtlinie (MDY-DEV-POL-02)**.

3.11. Compliance

monday.com verpflichtet sich, alle geltenden Gesetze, Vorschriften und Standards einzuhalten. Dies geschieht durch kontinuierliche Identifizierung neuer lokaler und internationaler Gesetze, neuer Vorschriften und der Veröffentlichung neuer Standards.

4. Richtlinien-Lebenszyklus

4.1. Ergänzungen, Änderungen und Löschungen

- Änderungen an etablierten Richtlinien, Standards und Baselines sind bei Bedarf vorzunehmen.
- Jeder Antrag muss eine geschäftliche Begründung für die beantragte Änderung enthalten.
- Der VP Operations muss jeden Antrag prüfen und genehmigen/ablehnen.
- Das Sicherheitsteam ist dafür verantwortlich, dass alle relevanten Änderungen oder Ergänzungen an die Mitarbeiter des Unternehmens weitergegeben werden.

4.2. Überprüfungsprozess

- Die globale Informationssicherheitsrichtlinie muss jährlich oder bei Bedarf in Übereinstimmung mit den geschäftlichen oder gesetzlichen Anforderungen überprüft und aktualisiert werden.
- Die Informationssicherheitsrichtlinien, -standards und -grundlagen müssen mindestens alle 12 Monate überprüft werden, um sicherzustellen, dass sie kohärent sind und Folgendes berücksichtigen:
    - Geschäftsanforderungen und Geschäftsumfeld – die Kontrollen müssen sowohl unter Kostengesichtspunkten als auch im Hinblick auf den laufenden Betrieb effizient bleiben und das Geschäft unterstützen, ohne dessen Abläufe unangemessen zu beeinträchtigen.
    - Externes technologisches Umfeld – Chancen und Gefahren, die sich aus Veränderungen, Trends und neuen Entwicklungen ergeben.
    - Internes technologisches Umfeld – Stärken und Schwächen, die sich aus der Nutzung der Technologie durch das Unternehmen ergeben.
    - Rechtliche, regulatorische und vertragliche Anforderungen.
    - Andere Anforderungen, die sich aus neuen oder einzigartigen Umständen ergeben.

4.3. Befugnisübertragung

- Der CISO kann bei Bedarf bestimmte Aufgaben und Zuständigkeiten an einzelne Mitarbeiter oder Referate delegieren.
- Delegierte Zuständigkeiten sind nicht übertragbar.

4.4. Ausnahmen von Richtlinien

- Die Mitarbeiter des Unternehmens und Dritte sind verpflichtet, die genannten Richtlinien und Standards einzuhalten.

- Sollte eine Richtlinie oder ein Standard nicht eingehalten werden können, muss der CISO eine Ausnahme von einer solchen Basislinie in Betracht ziehen.
- Eine Ausnahme darf nur dann gewährt werden, wenn die Vorteile der Ausnahme die sich daraus ergebenden Risiken überwiegen, wie vom CISO auf der Grundlage der Empfehlung des Sicherheitsforums festgestellt.
- Ausnahmen sind gegebenenfalls mit Fälligkeitsterminen zu versehen, um die rechtzeitige Umsetzung der vereinbarten Sanierungsstrategien zu gewährleisten.
- Die Ausnahmen müssen regelmäßig überprüft werden, um sicherzustellen, dass die Abhilfemaßnahmen fristgerecht durchgeführt werden.