# グローバル情報セキュリティポリシー

## MDY-ORG-POL-01

| | |
|---|---|
| コード | MDY-ORG-POL-01 |
| バージョン | 2.2 |
| 改訂日 | 2021年11月 |
| 作成／更新者 | Nitsan Tahal Bartov |
| 承認者 | Ouriel Weisz |
| 機密レベル | 公開 |

変更履歴：

| 日付 | バージョン | 作成者 | 承認者 | 変更内容 |
|---|---|---|---|---|
| 2017年11月 | 1.0 | Yaniv Milhovitch | Ouriel Weisz | 初版 |
| 2018年6月 | 1.1 | Ouriel Weisz | Ouriel Weisz | 改定、要約の追加 |
| 2019年1月 | 1.2 | Alex Barkin | Ouriel Weisz | 定期レビュー・改定 |
| 2019年12月 | 2.0 | Yuval Yelin | Shiran Nawi | 内容変更、ISMS準拠 |
| 2020年12月 | 2.1 | Mor Bouganim-Fogel | Ouriel Weisz | 定期レビュー・改定 |
| 2021年11月 | 2.2 | Nitsan Tahal Bartov | Ouriel Weisz | 定期レビュー・改定 |

# 目次

# 1. はじめに

## 1.1. 目的

グローバル情報セキュリティポリシー（GISP）の目的は、monday.comが自社およびお客様の情報を保護し、国内および国際的な法律、基準、規制を順守するために導入する対策および統制手段を定めることにあります。
GISPは、全ての従業員および契約相手が基準とすべき核となるポリシードキュメントであり、全てのユーザーが従うべき行動および禁止事項が定められています。

## 1.2. 適用範囲

本ポリシーは、monday.comの全ての情報を適用範囲とします。これには顧客情報、ソースコード、図表、財務情報、PII（個人を特定できる情報）およびPHI（保護対象保健情報）（該当する場合）が含まれます。

本ポリシーは、monday.comの組織全体を適用範囲とします。これにはその子会社、従業員、契約相手、下請け業者、パートナーならびにmonday.comの情報を作成、保持、保管、保有、送信し、またはこれにアクセスする全ての者が含まれます。

## 1.3. 定義

**CEO**：最高経営責任者は、プライバシーおよびセキュリティに関する当社の取り組み全般について責任を負います。

**CISO**：最高情報セキュリティ責任者は、当社の情報セキュリティに関する全ての事項について責任を負います。

**DPO**：データ保護責任者は、適切な個人データ保護措置が導入されていることを確認し、当社の製品および業務についてプライバシーの観点から監督する責任を負います。

**機密性**：情報が権限を有する者にのみ提供または開示されること。

**完全性**：全ての情報資産が正確かつ完全であること。

**可用性**：全ての情報が必要に応じてアクセス可能かつ利用可能であること。

**暗号化**：その情報を「知る必要（need to know）」を明確に有する者以外は読めない状態にするために、アルゴリズムを使って情報を変換するプロセス。

**個人を特定できる情報（PII）**：名前、識別番号、生年月日、出生地、生体データの記録、医療情報、資産に関する情報など、個人の身元を区別または追跡するために利用可能な個人に関するあらゆる情報。

**サードパーティ**：全てのベンダー、下請け業者およびmonday.comと契約関係にあるその他全ての者。

## 1.4. 情報セキュリティの目的

- monday.comの経営目標に沿って、これらの目標を達成するための当社の取り組みを支えます。
- セキュリティに関する全ての取り組みが、急速に成長する公開会社としての当社の義務と整合性が取れたものとなるよう万全を期します。
- 情報セキュリティリスクを軽減するため、包括的で最新の情報セキュリティ計画を整備します。
- セキュリティインシデントを最も初期の段階で防止し、セキュリティインシデントが発生した場合は、できるだけ早くこれを検知し、封じ込めます。

- 全ての資産およびその関連リスクをリスト化し、最新の状態に保ちます。

## 1.5. 情報セキュリティのための組織

monday.comのCISOは、当社の情報セキュリティ全般について責任を負います。

当社の業務について指示を出し、継続的に監視を行うため、少なくとも次の代表者が集まり、毎週セキュリティフォーラムを実施します。

- CISO
- オペレーション担当VP
- R&D部門情報セキュリティ責任者
- インフラ管理責任者
- インフラセキュリティ責任者
- ITマネージャー
- コンプライアンス専門家

必要に応じて、当社の各部門からその他の代表者がフォーラムに参加できます。

## 1.6. 情報セキュリティの管理

monday.comの従業員、契約相手およびサードパーティは全て、当社の各ポリシーに従い、オンボーディングの一環として、また日常的に、自らの責任を伝えられ、各ポリシーに24時間365日いつでもアクセスできるものとします。 ポリシーは全て、少なくとも年1回見直しが行われるものとします。当社の業務が大幅に変更され、当社またはお客様のデータの機密性、完全性または可用性に影響を及ぼす可能性がある場合は、該当するポリシーの見直しが実施されます。

ポリシーは全て、経営陣の1人により承認される必要があります。

### 1.7. 継続的改善

monday.comは、自社サービスに対する潜在的なリスクと保護措置の必要性を継続的に評価し、評価結果の深刻度に基づき修復戦略を策定します。

定期的に、以下の評価が実施されます。

- 脆弱性報奨金制度 - 継続的に実施
- アプリケーションの脆弱性検査 - 継続的に実施
- 重要な情報システムの総合的なリスク評価 - 年1回
- アプリケーションレベルのペネトレーションテスト - 年1回
- リスク管理プロセスの詳細については、**リスク管理ポリシー （MDY-ORG-POL-05）** をご覧ください。

## 2. 役割と責任

互いに相反する職務や責任範囲は切り離しを行い、組織の資産が権限なく、または意図せず改変・誤用される可能性を減らす必要があります。

### 2.1. 経営陣

当社の経営陣は、当社が本ポリシーを順守することについて総合的な責任を負います。

経営陣は、社内の情報セキュリティ管理システム（ISMS）を維持・改善するために十分なリソースを提供するものとします。

## 2.2. オペレーション担当VP

オペレーション担当VPは、セキュリティ予算の承認について責任を負います。

また、オペレーション担当VPは、サードパーティ（該当する場合）および経営陣の両者に対し、重要度の高いISMS活動（リスク対応計画、運用計画および目標など）の結果を伝えます。

## 2.3. CISO

CISOは、当社のセキュリティ戦略の策定、情報セキュリティプロセスの実装、統制およびその実施について責任を負います。　CISOは経営陣の監督下にあります。

CISOの主な責任は次のとおりです。

- 情報セキュリティ管理システム（ISMS）の文書類の所管
- セキュリティポリシーの一環として行われる定期リスク評価プロセスの指揮
- 状況に応じて、ポリシー、社内規定、手続きに対する変更の勧告
- 当社の全ての重要資産のセキュリティ確保および管理の徹底
- 情報セキュリティ教育、トレーニング、意識啓発プログラムの開発・維持
- 法律、規制、ベストプラクティス、フレームワークの順守に関する助言
- セキュリティ関連予算および投資計画の策定

## 2.4. セキュリティ運営委員会

セキュリティ運営委員会は、セキュリティ戦略計画の確認と承認について責任を負います。セキュリティ運営委員会は、年1回招集されます。

セキュリティ運営委員会は、次のメンバーで構成されます。

- CEO
- CTO
- オペレーション担当VP
- R&D担当VP
- ゼネラルカウンシル
- CISO

## 2.5. 情報セキュリティフォーラム

情報セキュリティフォーラムは、全ての情報セキュリティ活動について運用面の調整を行うフォーラムです。

その責任は次のとおりです。

- 情報管理手法（ポリシー、社内規定、ガイドライン、手続きを含む）の開発および実施の調整
- 当社の製品、コードおよびインフラに内在するセキュリティ関連の問題に関する開発・実装の調整
- 当社の従業員、ベンダー、パートナーおよびお客様から報告された現在発生しているセキュリティ関連の問題への対応
- 情報セキュリティ管理活動を組織全体で一貫性をもって実施できるよう、フォーラムのメンバー間で調整および情報共有

当社のセキュリティフォーラムは、少なくとも月1回招集されます。

## 2.6. 資産管理責任者

資産管理責任者とは、特に重要な資産の保護について説明責任を負うマネージャーのことを指します。資産管理責任者は、情報セキュリティに関する職務を他の個人に委任することができますが、職務の適切な実施について引き続き説明責任を負います。情報資産管理責任者の責任は次のとおりです。

- 情報資産の適切な分類および保護
- 適切な保護管理措置の特定と資金調達
- 分類およびビジネス上のニーズに従い、情報資産へのアクセスを承認
- 定期的なシステムアクセスレビュー／データアクセスレビューの速やかな実施
- 管理対象資産に関係する保護要件の順守状況の監視

## 2.7. 従業員

従業員は全員、情報セキュリティに関する当社のポリシーおよび社内規定を順守することが求められており、**利用規定**（MDY-ORG-POL-02）に従って当社の資産を利用するものとします。

# 3. 情報セキュリティの実装

## 3.1. 人的資源のセキュリティ

当社の従業員は、当社が保有する最も貴重なリソースの1つです。従業員は、業務上の理由で機微な情報にアクセスします。monday.comの人的資源を確実に管理することは、会社全体のセキュリティを確保する上で必要不可欠であり、人的資源のセキュリティに関するポリシー（**MDY-HR-POL-01**）で取り扱われています。

## 3.2. 資産管理のセキュリティ

組織内にある攻撃対象に関する知識不足や認識不足は、重大なリスクをもたらします。組織内にある資産の情報を整理し、セキュリティ対策を決定することで、組織のリスクレベルを大幅に低減させることができます。

- 当社の資産（データ、ソフトウェア、ハードウェアなど）は全て記録・報告され、管理責任者が指定されます。
- 全ての資産について資産管理責任者が特定され、担当資産の維持・保護について責任を負います。
- 情報は全て、データ分類ポリシー（MDY-ORG-POL-04）で詳述する機密レベルに応じて分類し、取り扱う必要があります。
- 資産管理のセキュリティについては、資産管理ポリシー（MDY-IT-POL-02）で詳しく定められています。

## 3.3. アクセス制御

資産へのアクセスは、組織において最も機微なプロセスの1つです。リソースに対するアクセス権の運用が適切に行われなかった場合、組織に重大なリスクをもたらします。

monday.comでは、知る必要（need-to-know）と最小権限の原則（least privilege principles）に従ってアクセス権が付与されます。アクセス制御のセキュリティに関する事項は、全てアクセス制御ポリシー（MDY-IT-POL-01）で詳しく記載されています。

## 3.4. 暗号

monday.comは、社内業務に関する情報に加え、機微な情報をお客様に代わって管理します。これらのデータを転送中（1つのコンポーネントから別のコンポーネントに送信する間）および保管中に暗号化することは極めて重要です。monday.comにおける暗号化によるセキュリティ管理の詳細は、暗号化の利用に関するポリシー（**MDY-IT-POL-04**）に記載されています。

## 3.5. 物理的・環境的セキュリティ

物理的・環境的セキュリティとは、monday.comが自社の物理的な施設や資産のセキュリティを確保するために利用する手段のことを指します。詳細は、物理的・環境的セキュリティに関するポリシー（**MDY-PHY-POL-01**）に記載されています。

## 3.6. 運用のセキュリティ

既存システムのキャパシティ管理と社内の新規システムの承認プロセスは、当社のポリシーに従って実施されるものとします。変更を適切に管理するため、変更管理プロセスが導入されています。詳細については、当社の**IT変更管理手続き（MDY-IT-PRD-01）**を参照してください。

monday.comがお客様に代わって取り扱う情報の喪失を防ぐため、バックアップを取り、合意済みのポリシーに従って定期的にテストを行うものとします。詳細は、バックアップポリシー（**MDY-IT-POL-05**）に記載されています。

## 3.7. 通信のセキュリティ

通信のセキュリティでは、転送中の情報（1つのITエンティティから別のエンティティに送信される情報）に対する不正アクセスの防止が問題になります。

通信のセキュリティは、物理的・環境的セキュリティに関するポリシー（MDY-PHY-POL-01）および暗号化の利用に関するポリシー（MDY-IT-POL-04）の両方で取り扱われています。

## 3.8. サプライチェーンのセキュリティ

monday.comでは、自社のサービスの一部について、サードパーティソリューションを利用しています。このサードパーティとの関係には、クラウドサービスプロバイダー、外部委託先、リモートサポートなどとの関係が含まれる可能性があります。サードパーティソリューションを導入する際は、当該サードパーティがmonday.comのリスクレベルに悪影響を及ぼさないよう、一定のセキュリティ対策を講じるものとします。

サプライチェーンのセキュリティは、サードパーティセキュリティポリシー（MDY-IT-POL-06）で取り扱われています。

## 3.9. 情報セキュリティインシデント管理、事業継続計画（BCP）、災害復旧計画（DRP）

monday.comでは、お客様に代わって処理するデータの機密性、可用性および完全性に影響を及ぼし得るインシデントを防ぐため、相当な努力を行っていますが、インシデントのリスクを完全に軽減することは不可能です。情報セキュリティインシデントが発生した場合、monday.comはできるだけ短期間でインシデントを検知し、封じ込めを行います。情報セキュリティインシデントの取り扱いに関する事項は、全て情報セキュリティおよびデータインシデント対応手続き（DOC-15）、災害復旧計画（DRP）（MDY-ORG-POL-03）および事業継続計画（BCP）（MDY-BCP-PLN-01）で取り扱われています。

## 3.10. 製品のセキュリティと安全な開発

monday.comのサービスでは、monday.comのお客様に代わって機微な重要データが処理されます。したがって、当社のサービスは、情報の機密性、可用性および完全性を確保するため、最高のセキュリティ水準に従って開発が行われるものとします。monady.comの安全な開発に関する取り組みおよび脆弱性管理の詳細については、**S-SDLC（セキュアソフトウェア開発ライフサイクル）ポリシー（MDY-DEV-POL-01）**および**パッチ管理ポリシー（MDY-DEV-POL-02）**を参照してください。

### 3.11. 順守

monday.comは、適用される全ての法律、規制および基準を順守すべく取り組んでいます。その実現のため、新しい国内法や国際法、規制、そして新たに公表される基準を継続的に確認します。

# 4. ポリシーのライフサイクル

## 4.1. 追加、変更、削除

- 制定されたポリシー、社内規定および基準は、必要に応じて変更するものとします。
- 申請を行う場合は、必ずその変更を申請するビジネス上の理由を記入する必要があります。
- オペレーション担当VPが、申請内容を確認して、承認または却下の判断を下すものとします。
- セキュリティチームは、変更または追加された内容を関係する全ての当社従業員に伝達する責任を負います。

## 4.2. レビュープロセス

- グローバル情報セキュリティポリシーは、毎年または必要に応じて、事業上または法規制上の要件に従い見直しと更新を行うものとします。
- 情報セキュリティに関するポリシー、社内規定および基準は、その内容に矛盾がないことを確認し、以下の事項に適切に対応するため、少なくとも12か月ごとに見直しを行うものとします。
    - 事業上のニーズおよび事業環境 – 内部統制は、コストおよび継続的な運用という2つの観点から有効なものでなければならず、事業プロセスを不合理に混乱させることなく、事業を下支えするものでなければなりません。
    - テクノロジーに関する外部環境 – 変化やトレンド、新たな展開により生まれる機会と脅威
    - テクノロジーに関する内部環境 – 当社がテクノロジーを利用することによって生じる強みと弱み
    - 法律、規制および規制に基づく要求事項
    - 新しい状況または独自の状況に固有のその他の要件

## 4.3. 責任の委譲

- CISOは、必要に応じて、一部の役割および責任を特定の従業員または部署に委譲することができます。
- 委譲された責任を委譲することはできません。

## 4.4. ポリシーに対する例外措置

- 会社の従業員およびサードパーティは、上述の各種ポリシーおよび社内規定を順守することが求められます。
- ポリシーまたは社内規定に従うことが不可能な場合、CISOは当該基準に対する例外措置を検討するものとします。

- 例外措置が認められるのは、例外措置の利益がリスクを上回る場合のみであり、これはセキュリティフォーラムの勧告に基づき、CISOが判断します。
- 該当する場合は、合意された修復戦略が速やかに実行されるよう、例外措置の期限を指定するものとします。
- 例外措置は、修復が期限内に完了することを確認するため、定期的に見直しを行うものとします。

**免責条項：このバージョンは、英語の原文を翻訳したものであり、便宜上の目的でのみ提供されています。この英語の原文は、正式な法的拘束力のあるバージョンであり、矛盾が生じた場合には英語の原文が優先されるものとします。**