Politique mondiale de sécurité des informations

MDY-ORG-POL-01

Code	MDY-ORG-POL-01
Version	2.2
Date de la version	Nov. 2021
Créée/mise à jour par	Nitsan Tahal Bartov
Approuvée par	Ouriel Weisz
Niveau de confidentialité	Public

Table des matières

1. Introduction

1.1. Objet

L'objectif de la politique mondiale de sécurité des informations (PMSI) est de définir les mesures et les contrôles mis en place par monday.com afin de protéger ses informations et celles de ses clients, et de se conformer aux lois, normes et réglementations locales et internationales.
Elle sert de document réglementaire central que tous les employés et sous-traitants doivent respecter et définit les actions et interdictions s'imposant à tous les utilisateurs.

1.2. Champ d'application

La présente politique s'applique à toutes les informations de monday.com, y compris les renseignements sur les clients, le code source, les diagrammes, les informations financières, les informations personnellement identifiables (IPI) et les informations médicales confidentielles (IMC) (le cas échéant).

Cette politique s'applique à l'ensemble de l'organisation monday.com, y compris ses filiales, employés, entrepreneurs, sous-traitants, partenaires et toute personne qui crée, entretient, stocke, accède à, traite ou transmet des informations monday.com.

1.3. Définitions

CEO : le Chief Executive Officer est responsable des pratiques générales de confidentialité et de sécurité de l'entreprise.

CISO : le Chief Information Security Officer est responsable de tous les aspects liés à la sécurité des informations de l'entreprise.

DPO : le Data Protection Officer est chargé de veiller à ce que des mesures de protection appropriées des données personnelles soient mises en place et de superviser tout ce qui touche à la confidentialité des produits et des pratiques de l'entreprise.

Confidentialité : les informations sont disponibles ou divulguées seulement aux personnes autorisées à en prendre connaissance.

Intégrité : toutes les ressources informationnelles sont exactes et complètes.

Disponibilité : toutes les informations sont accessibles et utilisables sur demande.

Chiffrement : processus de transformation des informations à l'aide d'un algorithme pour les rendre illisibles pour quiconque autre que ceux qui ont un « besoin de les connaître » spécifique.

Informations personnellement identifiables (IPI) : toute information sur une personne pouvant être utilisée pour distinguer ou tracer son identité, comme le nom, le numéro d'identification, la date et le lieu de naissance, les enregistrements biométriques, les informations médicales, les informations financières, etc.

Tierce partie : tous les fournisseurs, sous-traitants et autres parties sous contrat avec monday.com.

1.4. Objectifs de la sécurité des informations

- S'aligner sur les objectifs opérationnels de monday.com et soutenir les efforts de l'entreprise pour atteindre ceux-ci ;
- Veiller à ce que tous les efforts de sécurité soient alignés sur les obligations de l'entreprise en tant qu'entreprise publique, ainsi que sur son rythme de croissance rapide.
- Avoir en place un plan de sécurité des informations complet et à jour afin d'atténuer les risques liés à la sécurité des informations ;
- Prévenir les incidents en matière de sécurité le plus précocement possible et, s'ils se produisent, les détecter et les contenir au plus tôt ;
- Tenir à jour une liste de toutes les ressources et des risques qui y sont associés.

1.5. Organisation de la sécurité des informations

Le CISO de monday.com est responsable de la sécurité des informations de l'entreprise.

Afin de fournir des conseils et d'appliquer une surveillance continue des pratiques de l'entreprise, les représentants suivants, au minimum, seront tenus d'organiser chaque semaine une réunion du groupe chargé de la sécurité :

- CISO
- VP en charge des opérations
- Responsable R et D de la sécurité des informations
- Responsable de l'infrastructure
- Responsable de la sécurité de l'infrastructure
- Responsable des systèmes informatiques
- Spécialiste de la conformité

D'autres représentants des services de l'entreprise pourront se joindre au groupe au besoin.

1.6. Gestion de la sécurité des informations

Les employés, sous-traitants et tierces parties de monday.com doivent se conformer aux politiques de l'entreprise. Leurs responsabilités doivent leur être communiquées dans le cadre de leur intégration à l'entreprise et sur une base régulière. Ils doivent en outre disposer d'un accès 24 heures/24 et 7 jours/7 aux politiques. Toutes les politiques doivent être révisées au moins une fois par an. Les politiques applicables devront être examinées chaque fois qu'un changement majeur dans les pratiques de l'entreprise peut affecter la confidentialité, l'intégrité ou la disponibilité des données de l'entreprise ou de ses clients.

Toutes les politiques doivent être approuvées par un membre de la haute direction.

1.7. Amélioration continue

monday.com évalue en permanence les risques potentiels pour son service et évalue le besoin de mesures de protection, en se fondant sur sa stratégie de rectification en fonction de la gravité des constatations.

Les évaluations périodiques suivantes sont effectuées :

- Programme de recherche des bogues - sur une base continue
- Détection de la vulnérabilité des applications - sur une base continue
- Une évaluation globale des risques pesant sur les systèmes d'information critiques - sur une base annuelle
- Tests de pénétration au niveau des applications - sur une base annuelle
- Pour plus d'informations sur le processus de gestion des risques, veuillez consulter la **politique de gestion des risques (MDY-ORG-POL-05)**.

2. Rôles et responsabilités

Les tâches et les domaines de responsabilités entrant en conflit doivent être séparés afin de réduire les possibilités de modification ou d'utilisation abusive non autorisée ou non intentionnelle des ressources de l'organisation.

2.1. Équipe de direction

L'équipe de direction a la responsabilité globale de s'assurer que l'engagement de l'entreprise envers cette politique est respecté.

L'équipe de direction doit fournir les ressources nécessaires pour maintenir et améliorer le système de gestion de la sécurité des informations (SGSI) au sein de l'entreprise.

2.2. VP en charge des opérations

Le VP en charge des opérations est responsable de l'approbation des budgets liés à la sécurité.

En outre, le VP en charge des opérations communique les résultats des activités essentielles du SGSI (telles que l'évaluation des risques, le plan de traitement des risques, le plan opérationnel et les objectifs, etc.) aux tierces parties (le cas échéant) et à l'équipe de direction.

2.3. CISO

Le CISO est chargé de définir la stratégie de sécurité de l'entreprise, de mettre en œuvre les processus et les contrôles de sécurité des informations ainsi que leur application. Le CISO rend compte à l'équipe de direction.

Les principales responsabilités du CISO sont les suivantes :

- Chargé de la documentation du système de gestion de la sécurité des informations (SGSI).
- Direction du processus d'évaluation périodique des risques dans le cadre de la politique de sécurité.

- Le cas échéant, recommandation des modifications à apporter aux politiques, aux normes et aux procédures.
- Vérification que tous les actifs critiques de l'entreprise sont sécurisés et contrôlés.
- Élaboration et application d'un programme d'éducation, de formation et de sensibilisation à la sécurité des informations.
- Recommandations concernant la conformité aux lois, aux règlements, aux meilleures pratiques et aux cadres.
- Établissement d'un budget et de plans d'investissement liés à la sécurité.

2.4. Comité directeur en matière de sécurité

Le comité directeur en matière de sécurité est chargé d'examiner la planification stratégique en la matière et de l'approuver. Le comité directeur en matière de sécurité se réunira une fois par an.

Les membres du comité directeur en matière de sécurité sont :

- CEO
- CTO
- VP en charge des opérations
- VP en charge de la R et D
- Directeur juridique
- CISO

2.5. Groupe chargé de la sécurité des informations

Le groupe chargé de la sécurité est le groupe opérationnel pour toutes les activités liées à la sécurité des informations.

Ses responsabilités sont les suivantes :

- Coordonner l'élaboration et la mise en œuvre de pratiques de gestion des informations, y compris les politiques, les normes, les lignes directrices et les procédures ;
- Coordonner le développement et la mise en œuvre des questions de sécurité dans les produits, le code et l'infrastructure de l'entreprise ;
- Résoudre les problèmes de sécurité en cours soulevés par les employés, les fournisseurs, les partenaires et les clients de l'entreprise ;
- Coordonner et partager les informations parmi les membres du groupe afin d'assurer une exécution uniforme des activités de gestion de la sécurité des informations dans l'ensemble de l'organisation.

Le groupe chargé de la sécurité de l'entreprise se réunira au moins une fois par mois.

2.6. Titulaire de ressources

Les titulaires de ressources sont des gestionnaires tenus responsables de la protection de ressources importantes particulières. Ils peuvent déléguer des tâches en matière de sécurité des informations à d'autres personnes, mais restent responsables de la mise en œuvre appropriée de celles-ci. Les titulaires de ressources informationnelles sont responsables de ce qui suit :

- Classification et protection appropriées des ressources informationnelles ;
- Définition et financement des moyens de contrôle de protection appropriés ;
- Autorisation de l'accès aux ressources informationnelles en fonction de la classification et des besoins de l'entreprise ;
- Vérification que les examens réguliers du système/de l'accès aux données sont effectués en temps opportun ;

- Surveillance de la conformité aux exigences de protection affectant leurs ressources.

2.7. Employés

Tous les employés sont tenus de se conformer aux politiques et aux normes de sécurité des informations de l'entreprise et doivent utiliser les ressources de cette dernière conformément à la **politique d'utilisation acceptable (**MDY-ORG-POL-02**)**.

3. Mise en œuvre de la sécurité des informations

3.1. Sécurité des ressources humaines

Les employés d'une entreprise sont l'une des ressources les plus précieuses dont elle dispose. Les employés ont accès à des informations sensibles en raison de leur travail. La gestion sécurisée des ressources humaines de monday.com est un élément essentiel de la sécurité globale de l'entreprise et est couverte par la **politique de sécurité des RH (MDY-HR-POL-01)**.

3.2. Sécurité de la gestion des ressources

Le manque de connaissances et de compétences en ce qui concerne les cibles d'une attaque dans une organisation présente un risque important. La cartographie des ressources d'une organisation et la définition des mesures pour les sécuriser diminuent considérablement le niveau de risque s'y rapportant.

- Toutes les ressources de l'entreprise (telles que les données, les logiciels, le matériel, etc.) seront comptabilisées et auront un titulaire ;
- Les titulaires de ressources seront identifiés pour chacune d'elles et seront responsables de l'entretien et de la protection de leurs ressources ;

- Toutes les informations doivent être classées et traitées selon leurs niveaux de sensibilité, comme indiqué dans la **politique de classification des données (MDY-ORG-POL-04)**.
- La sécurité de la gestion des ressources est détaillée dans la **politique de gestion des ressources (MDY-IT-POL-02)**.

3.3. Contrôle d'accès

L'accès aux ressources est l'un des processus les plus sensibles d'une entreprise. Le fait de ne pas respecter les privilèges d'accès appropriés aux ressources peut exposer l'entreprise à un risque important.

Dans monday.com, les privilèges d'accès sont fournis selon les principes du besoin de savoir et du minimum de privilèges. Tous les aspects relatifs à la sécurité du contrôle d'accès sont détaillés dans la **politique du contrôle d'accès (MDY-IT-POL-01)**.

3.4. Cryptographie

monday.com gère des informations sensibles au nom de ses clients, en plus de celles relatives à ses opérations internes. Le chiffrement de ces données en transit (lorsqu'elles sont envoyées d'un composant à un autre) et au repos (lorsqu'elles sont stockées) est d'une importance cruciale. Les contrôles de sécurité cryptographiques de monday.com sont détaillés dans la **politique d'utilisation cryptographique (MDY-IT-POL-04)**.

3.5. Sécurité physique et environnementale

La sécurité physique et environnementale fait référence aux mesures que monday.com utilise pour sécuriser ses locaux et ses ressources. Elle est détaillée dans la **politique de sécurité physique et environnementale (MDY-PHY-POL-01)**.

3.6. Sécurité des opérations

La gestion de la capacité des systèmes existants et le processus d'acceptation de nouveaux systèmes au sein de l'entreprise doivent être conformes aux politiques de l'entreprise. Un processus de gestion des changements est en place pour garantir qu'ils sont contrôlés de façon pertinente. Pour plus d'informations, veuillez vous reporter à la **procédure de gestion des changements informatiques** de l'entreprise (**MDY-IT-PRD-01**).

Pour assurer la protection des informations que monday.com traite au nom de ses clients contre la perte, des sauvegardes doivent être effectuées et testées régulièrement conformément à une politique convenue, comme détaillé dans la **politique des sauvegardes (MDY-IT-POL-05)**.

3.7. Sécurité des communications

La sécurité des communications traite de la prévention de l'accès non autorisé aux informations en transit, à savoir celles qui sont envoyées d'une entité informatique à une autre.

La sécurité des communications est couverte à la fois par la **politique de sécurité physique et environnementale (MDY-PHY-POL-01)** et la **politique d'utilisation cryptographique (MDY-IT-POL-04)**.

3.8. Sécurité de la chaîne d'approvisionnement

monday.com utilise des solutions tierces pour certains aspects de son service. Ces relations avec des tiers peuvent inclure celles avec des fournisseurs de services dans le cloud, avec des sous-traitants externalisés, une assistance à distance, etc. Lors de la mise en œuvre d'une solution tierce, certaines mesures de sécurité doivent être prises afin de garantir que la tierce partie n'a pas d'impact négatif sur le niveau de risque encouru par monday.com.

La sécurité de la chaîne d'approvisionnement est couverte par la **politique de sécurité concernant les tierces parties (MDY-IT-POL-06)**.

3.9. Gestion des incidents affectant la sécurité des informations, plan de continuité des activités (PCA) et plan de reprise après sinistre (PRS)

monday.com déploie des efforts substantiels pour prévenir tout incident pouvant avoir un impact sur la confidentialité, la disponibilité et l'intégrité des données que l'entreprise traite au nom de ses clients. Malgré cela, il n'est pas possible d'atténuer pleinement le risque d'incidents. En cas d'incident lié à la sécurité des informations, monday.com le détectera et le contiendra dans les délais les plus courts possible. Tous les aspects de la gestion des incidents liés à la sécurité des informations sont traités dans la **procédure de réponse aux incidents liés à la sécurité et aux données** (interne), le **plan de reprise après sinistre (PRS) (MDY-ORG-POL-03)** et le **plan de continuité des activités (PCA)** (interne).

3.10. Sécurité des produits et développement sécurisé

Les services de monday.com traitent des données sensibles et critiques pour le compte de ses clients. Les services devraient donc être mis en place selon les normes de sécurité les plus élevées, afin d'assurer la confidentialité, la disponibilité et l'intégrité des informations. Pour en savoir plus sur les pratiques de développement sécurisé de monday.com et la gestion des vulnérabilités, veuillez vous reporter à la **politique S-SDLC (MDY-DEV-POL-01)** ainsi qu'à la **politique de gestion des correctifs (MDY-DEV-POL-02)**.

3.11. Conformité

monday.com s'engage à respecter toutes les lois, réglementations et normes applicables. Pour ce faire, il convient de prendre continuellement connaissance de nouvelles lois, de nouvelles réglementations et de la publication de nouvelles normes, tant au niveau local qu'international.

4. Cycle de vie des politiques

4.1. Ajouts, modifications et suppressions

- Des modifications doivent être apportées aux politiques, normes et bases de référence en cas de besoin.
- Chaque demande d'un tel changement doit inclure sa justification professionnelle.
- Le VP en charge des opérations doit examiner chaque demande pour l'approuver ou la refuser.
- L'équipe en charge de la sécurité est tenue de s'assurer que tous les changements ou ajouts pertinents sont communiqués aux employés de l'entreprise.

4.2. Processus de vérification

- La politique mondiale de sécurité des informations doit être examinée et mise à jour chaque année ou plus souvent si nécessaire, conformément aux exigences commerciales ou réglementaires.
- Les politiques, normes et bases de référence en matière de sécurité des informations doivent être examinées au moins tous les 12 mois afin de s'assurer qu'elles sont cohérentes et répondent correctement à ce qui suit :
    - Besoins et environnement de l'entreprise : les contrôles doivent rester efficaces tant du point de vue des coûts que de la continuité des opérations, et soutenir l'entreprise sans causer d'interruption déraisonnable de ses processus.
    - Environnement technologique externe : opportunités et menaces créées par les changements, les tendances et les nouveaux développements.

- Environnement technologique interne : forces et faiblesses résultant de l'utilisation de technologies par l'entreprise.
- Exigences légales, réglementaires et contractuelles.
- Autres exigences spécifiques aux circonstances nouvelles ou uniques.

4.3. Délégation des responsabilités

- Le CISO peut choisir de déléguer certains rôles et responsabilités à des employés ou services spécifiques, selon les besoins.
- Les responsabilités déléguées ne sont pas transférables.

4.4. Exception aux politiques

- Les employés de l'entreprise et les tierces parties sont tenus de se conformer aux politiques et normes en vigueur.
- Dans le cas où une politique ou une norme ne peut être respectée, une exception à une telle base de référence devrait être envisagée par le CISO.
- Une exception ne peut être accordée que si les avantages procurés par l'exception l'emportent sur les risques qui en découlent, tels que déterminés par le CISO sur recommandation du groupe chargé de la sécurité.
- Les exceptions doivent être associées à des dates d'échéance, le cas échéant, afin d'assurer la mise en œuvre en temps opportun des stratégies de rectification convenues.
- Les exceptions doivent être régulièrement examinées pour vérifier que des mesures correctives sont prises à temps.