Política Global de Segurança da Informação

MDY-ORG-POL-01

Código	MDY-ORG-POL-01
Versão	2.2
Data da versão	Novembro de 2021
Criada/atualizada por	Nitsan Tahal Bartov
Aprovada por	Ouriel Weisz
Nível de confidencialidade	Público

Histórico de alterações:

Data	Versão	Criada por	Aprovada por	Descrição da alteração
Novembro de 2017	1.0	Yaniv Milhovitch	Ouriel Weisz	Versão inicial
Junho de 2018	1.1	Ouriel Weisz	Ouriel Weisz	Revisões, resumo adicionado
Janeiro de 2019	1.2	Alex Barkin	Ouriel Weisz	Revisão periódica e retificação
Dezembro de 2019	2.0	Yuval Yelin	Shiran Nawi	Alteração de conteúdo. Conformidade com ISMS.
Dezembro de 2020	2.1	Mor Bouganim-Fogel	Ouriel Weisz	Revisão periódica e retificações
Novembro de 2021	2.2	Nitsan Tahal Bartov	Ouriel Weisz	Revisão periódica e retificações

Índice

1. Introdução

1.1. Finalidade

A finalidade da política global de segurança da informação (GISP) é definir as medidas e controles que a monday.com tem em vigor para proteger suas próprias informações e as informações de seus clientes, bem como cumprir a legislação, padrões e regulamentações locais e internacionais. Ela serve como um documento de política central, com o qual todos os funcionários e contratantes devem alinhar-se, e define ações e proibições que todos os usuários devem seguir.

1.2. Escopo

O escopo desta política são todas as informações da monday.com, incluindo informações de clientes, códigos-fonte, diagramas, informações financeiras, PII e PHI (quando aplicável).

O escopo desta política abrange a organização monday.com em sua integralidade, incluindo suas subsidiárias, funcionários, contratantes, subcontratantes, parceiros e qualquer pessoa que cria, mantém, armazena, acessa, processa ou transmite informações da monday.com.

1.3. Definições

CEO: o diretor executivo é responsável pelas práticas gerais de privacidade e segurança da empresa.

CISO: o diretor de segurança da informação é responsável por todos os aspectos de segurança das informações da empresa.

DPO: o diretor de proteção de dados é responsável por assegurar que estejam em vigor medidas protetivas adequadas para dados pessoais, além de supervisionar o aspecto de privacidade dos produtos e práticas da empresa.

Confidencialidade: a informação é disponibilizada ou divulgada somente para quem tenha autorização para recebê-la.

Integridade: todos os ativos de informações são precisos e completos.

Disponibilidade: todas as informações são acessíveis e usáveis sob demanda.

Criptografia: processo de transformação das informações usando um algoritmo que as torna ilegíveis por qualquer pessoa que não tenha a específica "necessidade de saber".

Informações de identificação pessoal (PII): qualquer informação sobre um indivíduo que possa ser usada para distingui-lo ou rastrear sua identidade, por exemplo, o nome, número de identificação, data e local de nascimento, registros biométricos, informações médicas, informações financeiras etc.

Terceiros: todos os fornecedores, subcontratantes e outras partes sob contrato com a monday.com.

1.4. Objetivos da segurança da informação

- Alinhar os objetivos de negócio da monday.com e respaldar os esforços da empresa para cumprir esses objetivos;
- Assegurar que todos os esforços de segurança estejam alinhados com as obrigações da empresa como sociedade de capital aberto e ao seu ritmo de crescimento acelerado.
- Manter um plano abrangente e atualizado de segurança da informação para mitigar os riscos que a ameaçam;
- Prevenir incidentes de segurança em seu estágio inicial, e, caso ocorram, detectá-los e contê-los o mais cedo possível;
- Manter uma lista atualizada de todos os ativos e riscos associados a eles.

1.5. Organização da segurança da informação

O CISO da monday.com tem responsabilidade geral sobre a segurança das informações da empresa.

Para oferecer orientação e monitoramento contínuo das práticas da empresa, os representantes a seguir organizam um fórum de segurança, no mínimo, uma vez por semana:

- CISO
- VP de operações
- Chefe de P&D em segurança da informação
- Chefe de infraestrutura
- Diretor de segurança de infraestrutura
- Gerente de TI
- Especialista em conformidade

Outros representantes dos departamentos da empresa podem participar do fórum, conforme necessário.

1.6. Gestão da segurança da informação

Todos os funcionários da monday.com, seus contratantes e terceiros devem cumprir as políticas da empresa, ter suas responsabilidades pertinentes comunicadas como parte de sua integração e de forma regular, além de terem acesso permanente às políticas. Todas as políticas devem ser revisadas pelo menos uma vez ao ano. Sempre que houver uma alteração substancial nas práticas da empresa que possa afetar a confidencialidade, integridade ou disponibilidade dos dados da empresa ou de seus clientes, as políticas aplicáveis serão revisadas.

Todas as políticas devem ser aprovadas por um membro da gestão sênior.

1.7. Melhorias contínuas

A monday.com analisa continuamente os riscos potenciais aos seus serviços e avalia a necessidade de medidas protetivas, baseando sua estratégia de reparação na gravidade das descobertas.

As seguintes avaliações periódicas são executadas:

- Programa de caça aos bugs – continuamente
- Varreduras de vulnerabilidades das aplicações – continuamente
- Avaliação geral de riscos dos sistemas de informação crítica – anualmente
- TP a nível de aplicativo – anualmente
- Para mais informações relacionadas ao processo de gestão de riscos, por favor, consulte a **política de gestão de riscos (MDY-ORG-POL-05)**.

2. Funções e responsabilidades

Deveres conflitantes e áreas de responsabilidades devem ser separados para reduzir as oportunidades de modificação não autorizada ou não intencional ou uso indevido dos ativos da organização.

2.1. Gestão sênior

A gestão sênior da empresa possui a responsabilidade geral de assegurar que o compromisso da empresa com esta política seja cumprido.

A gestão sênior deve fornecer recursos adequados para manter e aprimorar o sistema de gestão de segurança da informação (ISMS) dentro da empresa.

2.2. VP de operações

O VP de operações é responsável por aprovar os orçamentos de segurança.

Ademais, o VP de operações comunica os resultados das atividades essenciais do ISMS (por exemplo, avaliação de riscos, plano de tratamento de riscos, plano e metas operacionais etc.) tanto para terceiros (conforme aplicável) quanto para a gestão sênior.

2.3. CISO

O CISO é responsável por definir a estratégia de segurança da empresa, implementar os processos e controles de segurança da informação e executá-los. O CISO se reporta à gestão sênior.

As principais responsabilidades do CISO são:

- Propriedade da documentação do sistema de gestão de segurança da informação (ISMS).
- Liderar o processo de avaliação periódica de riscos como parte da política de segurança.
- Quando aplicável, recomendar alterações nas políticas, padrões e procedimentos.
- Assegurar que todos os ativos críticos da empresa estejam protegidos e controlados.
- Desenvolver e manter um programa de educação, treinamento e conscientização em segurança da informação.
- Aconselhar sobre a conformidade com a legislação, regulamentações, melhores práticas e frameworks.
- Desenvolver orçamentos e planos de investimento relacionados à segurança.

2.4. Comitê diretor de segurança

O comitê diretor de segurança é responsável por revisar o planejamento estratégico de segurança e aprová-lo. O comitê diretor de segurança se reunirá uma vez ao ano.

Os membros do comitê diretor de segurança são:

- CEO
- CTO
- VP de operações
- VP de P&D
- Conselho geral
- CISO

2.5. Fórum de segurança da informação

O fórum de segurança é o fórum operacional para todas as atividades de segurança da informação.

Suas responsabilidades são:

- Coordenar o desenvolvimento e a implementação das práticas de gestão da informação, incluindo políticas, padrões, diretrizes e procedimentos;
- Coordenar o desenvolvimento e a implementação de medidas contra problemas relacionados à segurança dos produtos, códigos e infraestrutura da empresa;
- Abordar de modo contínuo problemas relacionados à segurança, levantados por funcionários da empresa, fornecedores, parceiros e clientes;
- Coordenar e compartilhar informações entre os membros do fórum para assegurar a execução consistente das atividades de gestão de segurança da informação em toda a organização.

O fórum de segurança da empresa se reunirá, no mínimo, uma vez por mês.

2.6. Proprietário de ativos

Os proprietários de ativos são gerentes responsáveis pela proteção de ativos significativos e específicos. Eles podem delegar as tarefas de segurança da informação a outras pessoas, mas continuam responsáveis pela implementação adequada das tarefas. Os proprietários de ativos de informação são responsáveis por:

- Classificar e proteger adequadamente os ativos de informação;
- Especificar e financiar controles protetivos apropriados;
- Autorizar o acesso aos ativos de informação, de acordo com a classificação e as necessidades do negócio;
- Assegurar a realização oportuna de revisões regulares do sistema/dados;
- Monitorar a conformidade com os requisitos de proteção que afetam seus ativos.

2.7. Funcionários

Todos os funcionários são obrigados a cumprir as políticas e padrões de segurança da empresa e devem usar os ativos dela de acordo com a **política de uso aceitável (**MDY-ORG-POL-02**)**.

3. Implementação da segurança da informação

3.1. Segurança dos recursos humanos

Os funcionários de uma empresa são um de seus recursos mais valiosos. Eles têm acesso a informações sigilosas em virtude de sua função. Administrar com segurança os recursos humanos da monday.com é parte essencial da segurança geral da empresa e é coberta pela **política de segurança de RH (MDY-HR-POL-01)**.

3.2. Segurança da gestão de ativos

A falta de conhecimento e familiaridade com os alvos de ataques em uma organização representa um risco significativo. Mapear os ativos da organização e definir as medidas para protegê-los reduz substancialmente o nível de risco da organização.

- Todos os ativos da empresa (como dados, softwares, hardwares etc.) serão contabilizados e terão um proprietário;
- Os proprietários de ativos serão identificados para todos os ativos e serão responsáveis pela manutenção e proteção deles;
- Todas as informações devem ser classificadas e tratadas de acordo com seus níveis de sensibilidade, conforme detalhado na **política de classificação de dados (MDY-ORG-POL-04)**.
- A segurança da gestão de ativos é detalhada na **política de gestão de ativos (MDY-IT-POL-02)**.

3.3. Controle de acesso

O acesso aos ativos é um dos processos mais sensíveis em uma organização. A falha em manter os privilégios adequados de acesso aos recursos pode colocar a organização em risco significativo.

Os privilégios de acesso na monday.com são oferecidos de acordo com os princípios da necessidade de saber e do menor privilégio. Todos os aspectos da segurança do controle de acesso são detalhados na **política de controle de acesso (MDY-IT-POL-01)**.

3.4. Criptografia

A monday.com gerencia informações sigilosas em nome de seus clientes, além de informações pertinentes às suas operações internas. A criptografia desses dados tanto em trânsito (enquanto são enviadas de um componente para o outro) quanto em repouso (quando armazenados) é de fundamental importância. Os controles de segurança criptográficos da monday.com são detalhados na **política de uso criptográfico (MDY-IT-POL-04)**.

3.5. Segurança física e do ambiente

O aspecto de segurança física e do ambiente se refere às medidas que a monday.com utiliza para proteger suas instalações e ativos físicos. Ele é detalhado na **política de segurança física e do ambiente (MDY-PHY-POL-01)**.

3.6. Segurança de operações

A gestão de capacidade dos sistemas existentes e o processo para aceitar novos sistemas dentro da empresa devem ser realizados de acordo com as políticas da empresa. Um processo de gestão de mudanças está em vigor para assegurar que elas sejam bem-controladas. Para mais informações, por favor, consulte o **procedimento de gestão de mudanças em TI (MDY-IT-PRD-01)** da empresa.

Para garantir proteção contra a perda das informações tratadas pela monday.com em nome de seus clientes, backups serão realizados e testados regularmente, de acordo com a política acordada, conforme detalhado na **política de backup (MDY-IT-POL-05)**.

3.7. Segurança de comunicações

A segurança de comunicações lida com a prevenção do acesso não autorizado às informações em trânsito – informações que são enviadas de uma entidade de TI para outra.

A segurança de comunicações é coberta tanto pela **política de segurança física e do ambiente (MDY-PHY-POL-01)** quanto pela **política de uso criptográfico (MDY-IT-POL-04)**.

3.8. Segurança da cadeia de suprimento

A monday.com usa soluções terceirizadas para alguns aspectos de seus serviços. As respectivas relações com terceiros podem incluir provedores de serviços na nuvem, contratantes terceirizados, suporte remoto etc. Ao implementar uma solução terceirizada, algumas medidas de segurança devem ser adotadas para garantir que terceiros não afetem negativamente o nível de riscos da monday.com.

A segurança da cadeia de suprimento é coberta pela **política de segurança de terceiros (MDY-IT-POL-06)**.

3.9. Gestão de incidentes de segurança da informação, plano de continuidade dos negócios (BCP) e plano de recuperação de desastres (DRP)

A monday.com envida esforços substanciais para prevenir incidentes que possam afetar a confidencialidade, disponibilidade e integridade dos dados que processa em nome de seus clientes. Não obstante, não é possível mitigar completamente o risco de incidentes. Na hipótese de um incidente de segurança da informação, a monday.com detectará e fará a contenção do incidente no menor prazo possível. Todos os aspectos do tratamento de incidentes de segurança da informação são cobertos pelo **procedimento de resposta a incidentes de segurança da informação e dados (DOC-15)**, **plano de recuperação de desastres (DRP) (MDY-ORG-POL-03)** e **plano de continuidade dos negócios (BCP) (MDY-BCP-PLN-01)**.

3.10. Segurança de produto e desenvolvimento seguro

O serviço da monday.com processa dados sigilosos e críticos em nome de seus clientes. Portanto, o serviço deve ser desenvolvido com base nos mais altos padrões de segurança, a fim de garantir a confidencialidade, disponibilidade e integridade das informações. Para saber mais sobre a prática de desenvolvimento seguro da monday.com e sua gestão de vulnerabilidades, por favor, consulte a **política S-SDLC (MDY-DEV-POL-01)** e a **política de gestão de correções (MDY-DEV-POL-02)**.

3.11. Conformidade

A monday.com tem o compromisso de cumprir a legislação, regulamentações e padrões aplicáveis. Isso é feito através da contínua identificação de novas leis e regulamentações locais e internacionais, além da publicação de novos padrões.

4. Ciclo de vida da política

4.1. Adições, alterações e exclusões

- Conforme necessário, devem-se realizar alterações nas políticas, padrões e linhas de base estabelecidos.
- Cada solicitação deve incluir a justificativa de negócio para o pedido da respectiva alteração.
- O VP de operações deve analisar cada solicitação e aprová-la/reprová-la.
- A equipe de segurança é responsável por garantir que todas as alterações ou adições relevantes sejam comunicadas aos funcionários da empresa.

4.2. Processo de revisão

- A política global de segurança da informação deve ser revisada e atualizada anualmente ou quando necessário, de acordo com os requisitos comerciais ou regulatórios.
- As políticas, padrões e linhas de base de segurança da informação devem ser revisadas, no mínimo, a cada 12 meses, a fim de assegurar que sejam consistentes e abordem apropriadamente o seguinte:
    - Necessidades e ambiente de negócios – os controles devem continuar eficazes tanto da perspectiva de custos quanto de operação contínua, e respaldar os negócios sem causar interrupções desarrazoadas em seus processos.
    - Ambiente tecnológico externo – oportunidades e ameaças criadas por mudanças, tendências e novos desenvolvimentos.
    - Ambiente tecnológico interno – pontos fortes e fracos resultantes do uso de tecnologia pela empresa.
    - Requisitos legais, regulatórios e contratuais.
    - Outros requisitos específicos para circunstâncias novas ou únicas.

4.3. Delegação de responsabilidades

- O CISO pode optar por delegar algumas funções e responsabilidades para funcionários ou unidades específicas, conforme necessário.
- As responsabilidades delegadas são intransferíveis.

4.4. Exceção às políticas

- Os funcionários da empresa e terceiros são obrigados a cumprir todas as políticas e padrões.
- Na hipótese de não ser possível cumprir uma política ou padrão, o CISO deve considerar uma exceção à respectiva linha de base.

- Só se pode autorizar uma exceção se seus benefícios superarem os riscos resultantes, conforme determinado pelo CISO com base na recomendação do fórum de segurança.
- Deve-se atribuir prazo às exceções, quando aplicável, a fim de assegurar a implementação tempestiva das estratégias de reparação acordadas.

As exceções devem ser revisadas regularmente para confirmar se a reparação será realizada de forma oportuna. AVISO: Esta versão é uma tradução do original em inglês, fornecida apenas para fins de conveniência. O original em inglês é a versão oficial e juridicamente vinculante, e prevalecerá em caso de discrepância.