Política global de seguridad de la información

MDY-ORG-POL-01

Código	MDY-ORG-POL-01
Versión	2.2
Fecha de la versión	Nov 2021
Creada/actualizada por	Nitsan Tahal Bartov
Aprobada por	Ouriel Weisz
Nivel de confidencialidad	Público

Historial de cambios

Fecha	Versión	Creada por	Aprobada por	Descripción del cambio
Nov 2017	1.0	Yaniv Milhovitch	Ouriel Weisz	Versión inicial
Jun 2018	1.1	Ouriel Weisz	Ouriel Weisz	Revisiones, incorporación de resumen
Ene 2019	1.2	Alex Barkin	Ouriel Weisz	Correcciones y revisiones periódicas
Dic 2019	2.0	Yuval Yelin	Shiran Nawi	Cambio de contenidos. Cumplimiento con el ISMS
Dic 2020	2.1	Mor Bouganim-Fogel	Ouriel Weisz	Correcciones y revisiones periódicas
Nov 2021	2.2	Nitsan Tahal Bartov	Ouriel Weisz	Correcciones y revisiones periódicas

Índice

1. Introducción

1.1. Finalidad

La finalidad de la Política global de seguridad de la información (GISP) es definir las medidas y los controles con los que cuenta monday.com para proteger su información y la información de sus clientes, y cumplir con las leyes, normas y regulaciones locales e internacionales. Sirve como un documento normativo rector para todos los empleados y contratistas, y define las acciones y las prohibiciones que todos los usuarios deben cumplir.

1.2. Alcance

La presente política alcanza a toda la información de monday.com, que incluye la información del cliente, el código fuente, los diagramas, la información financiera, la información de identificación personal y la información médica protegida (si corresponde).

La presente política alcanza a toda la organización de monday.com, que incluye sus subsidiarias, empleados, contratistas, subcontratistas, socios y todo aquel que genere, mantenga, almacene, acceda, procese o transmita información de monday.com.

1.3. Definiciones

CEO: el Director ejecutivo es el responsable de las prácticas de privacidad y seguridad de la compañía en general.

CISO: el Oficial de seguridad de la información es el responsable de todos los aspectos de seguridad de la información de la compañía.

DPO: el Oficial de protección de datos es el responsable de garantizar que se apliquen las medidas de protección que competen a los datos personales y de supervisar el aspecto relativo a la privacidad de los productos y las prácticas de la compañía.

Confidencialidad: la información está a disposición de, o se comparte con, las personas autorizadas únicamente.

Integridad: todos los activos de información son precisos y completos.

Disponibilidad: toda la información está disponible y es utilizable bajo demanda.

Cifrado: el proceso de transformar la información mediante el uso de un algoritmo para hacerla ilegible a cualquier sujeto que no tenga una "necesidad específica de conocerla".

Información de identificación personal (IIP): cualquier información sobre un individuo que pudiera utilizarse para distinguir o rastrear su identidad, como su nombre, número de documento, la fecha y el lugar de nacimiento, los registros biométricos, la información médica, la información financiera, etc.

Terceros: todos los proveedores, subcontratistas y otros terceros con contrato con monday.com.

1.4. Objetivos de seguridad de la información

- Estar en consonancia con los objetivos comerciales de monday.com y contribuir a la realización de dichos objetivos;
- Procurar que todos los esfuerzos estén en consonancia con las obligaciones de la compañía en su calidad de entidad pública y acompañar su ritmo acelerado de crecimiento;
- Mantener un plan de seguridad de la información integral y actualizado para mitigar los riesgos relativos a la seguridad de la información;
- Prevenir los incidentes de seguridad en su etapa incipiente y, en caso de que ocurran, detectarlos y contenerlos con la mayor celeridad posible;
- Llevar una lista actualizada de todos los activos y los riesgos asociados a ellos.

1.5. Organización de la seguridad de la información

El CISO de monday.com carga con la responsabilidad general de la seguridad de la información de la compañía.

Con el fin de proporcionar pautas y llevar un seguimiento continuo de las prácticas de la compañía, los siguientes representantes conducen un Foro de Seguridad con una frecuencia semanal, como mínimo:

- CISO
- VP de operaciones
- Jefe de seguridad de la información de I+D
- Director de infraestructura
- Jefe de seguridad de la infraestructura
- Gerente de TI
- Especialista en cumplimiento

Otros representantes de los departamentos de la compañía podrán sumarse, de ser necesario.

1.6. Gestión de seguridad de la información

Todos los empleados, contratistas y terceros vinculados con monday.com deben adherir a las políticas de la compañía, ser informados periódicamente de las responsabilidades que les competen como parte de su incorporación y tener acceso a las políticas las 24 horas, todos los días. Todas las políticas deben revisarse, como mínimo, una vez al año. Siempre que haya un cambio sustancial a las prácticas de la compañía que pudiera afectar la confidencialidad, la integridad o la disponibilidad de los datos de la compañía o de sus clientes, se deberán revisar las políticas que correspondan.

Todas las políticas deben ser aprobadas por un miembro de la alta gerencia.

1.7. Mejoramiento continuo

monday.com evalúa continuamente los posibles riesgos en sus servicios y la necesidad de implementar medidas de protección, adecuando su estrategia de corrección a la gravedad de los acontecimientos.

Se ejecutan las siguientes evaluaciones periódicas:

- Programa de recompensas por errores - de manera continua
- Ejecución de análisis de vulnerabilidades - de manera continua
- Una evaluación general de riesgo de los sistemas de información crítica - anualmente
- Pruebas de penetración (PT) a nivel de aplicación - anualmente
- Para obtener más información sobre el procesos de Gestión de riesgos, consulte la **Política de gestión de riesgos (MDY-ORG-POL-05)**.

2. Funciones y responsabilidades

Las funciones y las áreas de responsabilidad incompatibles deben estar separadas a fin de reducir la posibilidad de cualquier modificación no autorizada o no intencionada, o el uso indebido de los activos de la organización.

2.1. Alta gerencia

La alta gerencia de la compañía tiene la responsabilidad general de garantizar que la compañía asuma el compromiso de cumplir con esta política.

La alta gerencia suministrará los recursos necesarios para el mantenimiento y el mejoramiento del Sistema de gestión de seguridad de la información (ISMS) dentro de la compañía.

2.2. VP de operaciones

El VP de operaciones es el responsable de aprobar los presupuestos destinados a la seguridad.

Además, el VP de operaciones se encarga de comunicar los resultados de las actividades esenciales del ISMS (como las evaluaciones de riesgos, el plan de tratamiento del riesgo, el plan y los objetivos operativos, etc.) tanto a terceros como a la alta gerencia.

2.3. CISO

El CISO es el responsable de definir la estrategia de seguridad de la compañía, como también la implementación de los procesos y controles de seguridad de la información y su cumplimiento. El CISO rinde cuentas a la alta gerencia.

Las responsabilidades principales del CISO son:

- Tener la propiedad de la documentación del Sistema de gestión de seguridad de la información (ISMS).
- Dirigir el proceso de las evaluaciones periódicas de riesgos como parte de la política de seguridad.
- Sugerir cambios a las políticas, las normas y los procedimientos, cuando corresponda.
- Garantizar que todos los activos críticos de la compañía estén protegidos y bajo control.
- Desarrollar e implementar un programa de educación, formación y concienciación sobre seguridad de la información.
- Ofrecer asesoría en cuanto al cumplimiento de las leyes, las normas, las mejores prácticas y los estándares de trabajo.
- Elaborar un presupuesto de seguridad y planes de inversión.

2.4. Comité directivo de seguridad

El comité directivo de seguridad es el responsable de revisar la planificación estratégica en materia de seguridad y de aprobarla. El comité directivo de seguridad se reunirá una vez al año.

Los miembros que componen el comité directivo de seguridad son:

- El CEO
- El CTO
- El VP de operaciones
- El VP de I+D
- El consejo general
- El CISO

2.5. Foro de seguridad de la información

El Foro de seguridad es un foro operativo que abarca todas las actividades de seguridad de la información.

Sus responsabilidades incluyen:

- Coordinar el desarrollo y la implementación de las prácticas relativas a la administración de la información, como las políticas, los estándares, las directivas y los procedimientos;
- Coordinar el desarrollo y la implementación de asuntos relativos a la seguridad en los productos, en el código y en la infraestructura de la compañía;
- Atender los problemas habituales relativos a la seguridad que plantean los empleados, los proveedores, los socios y los clientes de la compañía;
- Coordinar y compartir información entre los miembros del Foro para que haya una uniformidad en la ejecución de las actividades de administración de seguridad de la información a lo largo de toda la organización.

El Foro de seguridad de la compañía se reunirá, al menos, una vez al mes.

2.6. Propietario de activos

Los propietarios de activos son gerentes que tienen la responsabilidad de velar por la protección de determinados activos de importancia. Pueden delegar tareas de seguridad de la información en otros individuos, pero siguen siendo responsables de la debida implementación de las tareas. Los propietarios de activos de información tienen la responsabilidad de:

- Clasificar y proteger debidamente los activos de información;
- Especificar y financiar los controles de protección adecuados;
- Autorizar el acceso a los activos de información según su clasificación y necesidad comercial;
- Garantizar que las evaluaciones periódicas de acceso a los datos/sistemas se completen puntualmente;
- Supervisar que se cumpla con los requisitos de protección que incumben a los activos.

2.7. Empleados

Se exige que todos los empelados cumplan con las políticas y las normas relativas a la seguridad de la información de la compañía y que utilicen los activos de la compañía según lo estipulado en la **Política de uso aceptable** (**MDY-ORG-POL-02**).

3. Implementación de la seguridad de la información

3.1. Seguridad de los recursos humanos

Los empleados de la compañía son el activo más valioso. Dada la naturaleza de su trabajo, los empleados tienen acceso a información sensible. El manejo seguro de los recursos humanos de monday.com constituye una parte esencial de la seguridad general de la compañía y se aborda en la **Política de seguridad de recursos humanos (MDY-HR-POL-01)**.

3.2. Seguridad en la gestión de activos

Carecer de conocimientos y no estar familiarizado con los objetivos de ataque en una organización representa un riesgo sustancial. La elaboración de un esquema de los activos de una organización y la definición de medidas para protegerlos reduce de manera considerable el nivel de riesgo.

- Todos los activos de la compañía (como los datos, el software, el hardware, etc.) se contabilizarán y tendrán asignado un propietario;
- Se identificarán propietarios de activos para todos los activos, quienes serán responsables de su cuidado y mantenimiento;
- Toda la información se clasificará y se manejará de acuerdo con su nivel de sensibilidad, como se detalla en la **Política de clasificación de datos (MDY-ORG-POL-04)**.
- La seguridad en la gestión de activos se detalla en la **Política de gestión de activos (MDY-IT-POL-02)**.

3.3. Control de acceso

El acceso a los activos es uno de los procesos más delicados en una organización. No cumplir adecuadamente con los privilegios de acceso a los recursos puede poner en peligro a la organización.

En monday.com, los privilegios de acceso se otorgan de conformidad con los principios de necesidad de divulgación y de privilegios mínimos. Todos los aspectos relativos al control de acceso se detallan en la **Política de control de acceso (MDY-IT-POL-01)**.

3.4. Criptografía

monday.com gestiona información sensible en nombre de sus clientes, además de la información propia de sus operaciones internas. El cifrado de todos esos datos tanto en tránsito (al ser enviados de un componente a otro) como en reposo (al estar guardados) es de vital importancia. Los controles de seguridad criptográfica de monday.com se detallan en la **Política de uso de criptografía (MDY-IT-POL-04)**.

3.5. Seguridad física y ambiental

El aspecto relativo a la seguridad física y ambiental hace referencia a las medidas que aplica monday.com para cuidar de sus activos e instalaciones físicas, las cuales se detallan en la **Política de seguridad física y ambiental (MDY-PHY-POL-01)**.

3.6. Seguridad de las operaciones

La administración de la capacidad de los sistemas actuales y el proceso necesario para la aceptación de nuevos sistemas en la compañía deben realizarse de conformidad con las políticas de la compañía. Contamos con un proceso de administración de cambios para el control eficaz de estos. Para obtener más información, consulte el **Procedimiento de administración de cambios de TI (MDY-IT-PRD-01)** de la compañía.

Con el fin de garantizar la protección de la información que monday.com gestiona en nombre de sus clientes y evitar pérdidas, se seleccionarán y comprobarán copias de seguridad de forma periódica, conforme una política acordada, como se detalla en la **Política de copias de seguridad (MDY-IT-POL-05)**.

3.7. Seguridad de las comunicaciones

La seguridad de las comunicaciones abarca la prevención del acceso no autorizado a la información en tránsito; es decir, la información enviada desde una entidad de TI a otra.

La seguridad de las comunicaciones se aborda tanto en la **Política de seguridad física y ambiental (MDY-PHY-POL-01)** como en la **Política de uso de criptografía (MDY-IT-POL-04)**.

3.8. Seguridad en la cadena de suministro

monday.com utiliza soluciones de terceros para determinados aspectos de su servicio. Estas relaciones con terceros pueden incluir a proveedores de servicios de nube, contratistas externos, soporte remoto, etc. Al implementar soluciones de terceros, deben tomarse determinadas medidas de seguridad para que la intervención de esos terceros no afecte de forma negativa el nivel de riesgo de monday.com.

El tema de la cadena de suministro se aborda en la **Política de seguridad de terceros (MDY-IT-POL-06)**.

3.9. Administración de incidentes de seguridad de la información, Plan de Continuidad de la Actividad (BCP) y Plan de Recuperación de Desastres (DRP)

monday.com realiza importantes esfuerzos para prevenir cualquier incidente que pudiera afectar la confidencialidad, la disponibilidad y la integridad de los datos que procesa en nombre de sus clientes. Sin perjuicio de ello, es imposible evitar por completo el riesgo de incidentes. Ante la eventualidad de un incidente relacionado con la seguridad de la información, monday.com procurará detener y contener el incidente en el menor tiempo posible. Todos los aspectos sobre el manejo de los incidentes relacionados con la seguridad de la información se abordan en el **Procedimiento de respuesta a incidentes relativos a la seguridad de la información y los datos (DOC-15)**, el **Plan de Recuperación de Desastres (DRP) (MDY-ORG-POL-03)** y el **Plan de Continuidad de la Actividad (BCP) (MDY-BCP-PLN-01)**.

3.10. Seguridad del producto y desarrollo seguro

El servicio de monday.com procesa datos sensibles y críticos en nombre de sus clientes. En este sentido, el servicio debe desarrollarse manteniendo los más altos estándares en materia de seguridad, a los efectos de garantizar la confidencialidad, la disponibilidad y la integridad de la información. Para conocer más acerca de las prácticas de desarrollo seguro y la gestión de vulnerabilidades de monday.com, consulte la **Política de S-SDLC (MDY-DEV-POL-01)** y la **Política de gestión de revisiones (MDY-DEV-POL-02)**.

3.11. Cumplimiento

monday.com se compromete a cumplir con todas las leyes, normas y reglamentos vigentes, estando continuamente atentos a la promulgación de nuevas leyes locales e internacionales, los nuevos reglamentos y la publicación de nuevas normas.

4. Ciclo de vida de las políticas

4.1. Incorporaciones, cambios y eliminaciones

- Se realizarán modificaciones a las políticas, las normas y las directrices establecidas según sea necesario.
- Toda solicitud de tal índole debe incluir su debida justificación comercial.
- El VP de operaciones debe revisar cada solicitud y aprobarla o rechazarla.
- El equipo de Seguridad es el responsable de garantizar que se comuniquen a los empleados de la compañía todos los cambios o incorporaciones pertinentes.

4.2. Proceso de revisión

- La Política global de seguridad de la información debe revisarse y actualizarse anualmente o cuando fuera necesario, de conformidad con los requisitos comerciales o normativos.
- Las políticas, las normas y las directrices en materia de seguridad de la información deben revisarse, al menos, cada 12 meses para comprobar que estén en consonancia y que aborden adecuadamente lo siguiente:
    - Las necesidades comerciales y el entorno comercial – los controles deben mantener su eficacia, tanto en materia de costos como de las operaciones en curso, y ser de apoyo para la empresa sin provocar una alteración significativa en sus procesos.
    - El entorno tecnológico externo – oportunidades y amenazas originadas a partir de cambios, tendencias y nuevos desarrollos.
    - El entorno tecnológico interno – fortalezas y debilidades como consecuencia del uso que la compañía hace de la tecnología.
    - Requisitos legales, normativos y contractuales.
    - Otros requisitos específicos en lo que atañe a circunstancias nuevas o particulares.

4.3. Delegación de responsabilidades

- El CISO puede optar por delegar determinadas funciones y responsabilidades a empleados o unidades específicos, según la necesidad.
- Las responsabilidades que se delegan no se pueden transferir a otros.

4.4. Excepción a las políticas

- Los empleados de la Compañía y los terceros tienen la obligación de cumplir con las Políticas y Normas mencionadas.
- En caso de que no se pueda cumplir con una política o una norma, el CISO podrá considerar una excepción a dicha situación.
- La excepción solo podrá tener lugar cuando los beneficios que otorgue compensen los riesgos causados, según lo determine el CISO y considerando la recomendación del Foro de Seguridad.
- Siempre que corresponda, las excepciones tendrán asignada una fecha de caducidad a los efectos de garantizar la implementación oportuna de las estrategias de corrección acordadas.
- Las excepciones deben ser revisadas periódicamente para comprobar que la corrección se aplique de manera oportuna.