글로벌 정보 보안 정책

MDY-ORG-POL-01

코드	MDY-ORG-POL-01
버전	2.2
버전 날짜	2021년 11월
작성자/업데이트자	Nitsan Tahal Bartov
승인자	Ouriel Weisz
기밀 수준	공개

변경 내역:

날짜	버전	작성자	승인자	변경 설명
2017년 11월	1.0	Yaniv Milhovitch	Ouriel Weisz	초기 버전
2018년 6월	1.1	Ouriel Weisz	Ouriel Weisz	개정판, 요약 첨부
2019년 1월	1.2	Alex Barkin	Ouriel Weisz	정기 검토 및 수정
2019년 12월	2.0	Yuval Yelin	Shiran Nawi	내용 변경. ISMS 준수
2020년 12월	2.1	Mor Bouganim-Fogel	Ouriel Weisz	정기 검토 및 수정

2021년 11월	2.2	Nitsan Tahal Bartov	Ouriel Weisz	정기 검토 및 수정

목차

Contents

1. 소개

1.1. 목적

글로벌 정보 보안 정책(GISP)의 목적은 monday.com이 해당 정보와 고객 정보를 보호하고 현지 및 국제 법률과 표준 및 규정을 준수하기 위해 마련한 조치 및 통제를 정의하는 것입니다.
이는 모든 직원과 계약자가 준수해야 하는 중앙 정책 문서 역할을 하며 모든 사용자가 따라야 하는 조치 및 금지 사항을 정의합니다.

1.2. 범위

이 정책의 범위는 고객 정보, 소스 코드, 다이어그램, 재무 정보, PII 및 PHI(해당되는 경우)를 포함한 모든 monday.com 정보입니다.

이 정책의 범위는 자회사, 직원, 계약자, 하청 계약자, 파트너 및 monday.com의 정보를 생성, 유지 관리, 저장, 액세스, 처리 또는 전송하는 모든 사람을 포함한 전체 monday.com 조직입니다.

1.3. 정의

CEO: 최고 경영자는 회사의 전반적인 개인정보 보호 및 보안 측면을 책임집니다.

CISO: 최고 정보 보안 책임자는 회사의 모든 정보 보안 측면을 책임집니다.

DPO: 데이터 보호 책임자는 개인 데이터에 대한 적절한 보호 조치를 취하고 회사 제품 및 관행의 개인정보 보호 측면을 감독할 책임이 있습니다.

기밀 유지: 정보는 승인된 사람에게만 제공되거나 공개되어야 합니다.

무결성: 모든 정보 자산은 정확하고 완전해야 합니다.

유효성: 모든 정보는 요청 시 액세스 및 사용할 수 있어야 합니다.

암호화: 특정된 "알 필요"가 있는 사람 이외의 다른 사람이 읽을 수 없도록 알고리즘을 사용하여 정보를 변환하는 프로세스입니다.

개인 식별 정보(PII): 성명, 주민등록번호, 생년월일, 출생 장소, 생체 기록, 의료정보, 금융정보 등 개인을 식별하거나 추적할 수 있는 개인에 관한 모든 정보를 말합니다.

제삼자: monday.com과 계약을 체결한 모든 공급 업체, 하청 업체 및 기타 당사자를 말합니다.

1.4. 정보 보안 목표

- monday.com의 비즈니스 목표에 부합하고 이러한 목표를 달성하기 위한 회사의 노력을 지원합니다;
- 모든 보안 노력이 공개 기업으로서 회사의 의무 및 빠르게 성장하는 속도와 일치하는지 확인합니다.

- 정보 보안 위험을 완화하기 위해 포괄적이며 최신인 정보 보안 계획을 유지합니다;
- 보안 사고를 초기에 예방하고, 발생 시 조기에 탐지 및 억제합니다;
- 모든 자산의 최신 목록 및 이러한 자산과 관련된 위험을 관리합니다.

1.5. 정보 보안 조직

monday.com의 CISO는 회사의 정보 보안에 대한 전반적인 책임을 집니다.

회사의 관행에 대한 지침과 지속적인 모니터링을 제공하기 위해 다음 담당자는 최소한 매주 보안 포럼을 실시합니다:

- CISO
- VP 운영팀
- R&D 정보 보안 책임자
- 인프라 책임자
- 인프라 보안 책임자
- IT 관리자
- 규정 준수 전문가

필요에 따라 회사 부서의 추가 담당자가 포럼에 참여할 수 있습니다.

1.6. 정보 보안 관리

monday.com의 모든 직원, 계약자 및 제삼자는 회사의 정책을 준수하고, 온보딩의 일부로 정기적으로 관련 책임을 알려야 하며, 연중무휴 24시간 정책에 액세스할 수 있어야 합니다. 모든 정책은 최소한 매년 검토되어야 합니다. 회사 또는 고객 데이터의 기밀성, 무결성 또는 가용성에 영향을 미칠 수 있는 회사 관행에 중대한 변경이 있을 때마다 해당 정책이 검토되어야 합니다.

모든 정책은 고위 경영진의 승인을 받아야 합니다.

1.7. 지속적인 개선

monday.com은 서비스에 대한 잠재적 위험을 지속적으로 평가하고 조사 결과의 심각도에 따른 교정 전략을 기반으로 보호 조치의 필요성을 평가합니다.

다음과 같은 정기 평가가 실행됩니다:

- 버그 바운티 프로그램 - 지속적
- 애플리케이션 취약점 검사 - 지속적
- 중요 정보 시스템의 전반적인 위험 평가 - 매년
- 애플리케이션 수준 PT - 매년
- 위험 관리 프로세스에 대한 자세한 내용은 **위험 관리 정책 (MDY-ORG-POL-05)**을 참조하세요.

2. 역할과 책임

충돌하는 의무와 책임 영역은 조직 자산의 무단 또는 의도하지 않은 수정 또는 오용의 기회를 줄이기 위해 분리되어야 합니다.

2.1. 고위 경영진

회사의 고위 경영진은 이 정책에 대한 회사의 약속을 충족시킬 전반적인 책임이 있습니다.

고위 경영진은 회사 내 정보 보안 관리 시스템(ISMS)을 유지 관리하고 개선하기 위해 적절한 리소스를 제공해야 합니다.

2.2. VP 운영팀

VP 운영팀은 보안 예산 승인을 담당합니다.

또한 VP 운영팀은 필수 ISMS 활동(예: 위험 평가, 위험 처리 계획, 운영 계획 및 목표 등)의 결과를 제삼자(해당되는 경우)와 고위 경영진에게 전달합니다.

2.3. CISO

CISO는 회사의 보안 전략, 정보 보안 프로세스와 제어 구현 및 그 시행을 정의할 책임이 있습니다. CISO는 고위 경영진에게 보고합니다.

CISO의 주요 책임은 다음과 같습니다:

- 정보 보안 관리 시스템(ISMS) 문서의 소유권.

- 보안 정책의 일환으로 주기적인 위험 평가 프로세스 주도.
- 해당되는 경우 정책, 표준 및 절차에 대한 변경 권장.
- 모든 중요한 회사 자산 보호 및 통제.
- 정보 보안 교육, 훈련 및 인식 프로그램 개발 및 유지.
- 법률, 규정, 모범 사례 및 프레임워크 준수에 대해 조언.
- 보안 관련 예산 및 투자 계획 수립.

2.4. 보안 운영위원회

보안 운영 위원회는 보안 전략 계획을 심의하고 승인하는 역할을 한다. 보안 운영 위원회는 연 1회 개최됩니다.

보안 운영 위원회 위원은 다음과 같습니다:

- CEO
- CTO
- VP 운영팀
- VP R&D
- 법률 고문
- CISO

2.5. 정보 보안 포럼

보안 포럼은 모든 정보 보안 활동을 위한 운영 포럼입니다.

책임은 다음과 같다:

- 정책, 표준, 지침 및 절차를 포함한 정보 관리 관행의 개발 및 구현 조정;
- 회사 제품, 코드 및 인프라에서 보안 관련 문제의 개발 및 구현을 조정;
- 회사 직원, 공급 업체, 파트너 및 고객이 제기한 지속적인 보안 관련 문제 해결;
- 조직 전체에서 정보 보안 관리 활동의 일관된 실행을 보장하기 위해 포럼 회원 간의 정보 조정 및 공유.

회사의 보안 포럼은 적어도 한 달에 한 번 만날 것입니다.

2.6. 자산 소유자

자산 소유자는 중요한 특정 자산을 보호할 책임이 있는 관리자입니다. 그들은 정보 보안 작업을 다른 개인에게 위임할 수 있지만 작업의 적절한 구현에 대한 책임은 남아 있습니다. 정보 자산 소유자는 다음에 대한 책임이 있습니다:

- 정보 자산의 적절한 분류 및 보호
- 적절한 보호 통제 지정 및 자금 조달;
- 분류 및 비즈니스 요구에 따라 정보 자산에 대한 액세스 권한 부여;
- 정기적인 시스템/데이터 액세스 검토 적시 완료;
- 자산에 영향을 미치는 보호 요구 사항 준수 모니터링.

2.7. 직원

모든 직원은 회사의 정보 보안 정책 및 표준을 준수해야 하며 **사용 제한 정책** (MDY-ORG-POL-02)에 따라 회사 자산을 사용해야 합니다.

3. 정보 보안 구현

3.1. 인적 자원 보안

회사의 직원은 회사가 가진 가장 소중한 자원 중 하나입니다. 직원들은 업무상 민감한 정보에 접근할 수 있습니다. monday.com의 인적 자원을 안전하게 관리하는 것은 회사 전체 보안의 필수적인 부분이며 **인적 자원 보안 정책 (MDY-HR-POL-01)**에서 다루고 있습니다.

3.2. 자산 관리 보안

조직의 공격 대상에 대한 지식과 익숙한 자각이 부족하면 상당한 위험이 따릅니다. 반면 조직의 자산을 매핑하고 자산을 보호하기 위한 조치를 정의하면 조직의 위험 수준이 크게 낮아집니다.

- 모든 회사 자산(예: 데이터, 소프트웨어, 하드웨어 등)은 회계 처리되며 소유자가 있습니다;
- 자산 소유자는 모든 자산을 식별하며 자산의 유지 관리 및 보호에 대한 책임이 있습니다;

- 모든 정보는 **데이터 분류 정책 (MDY-ORG-POL-04)**에 자세히 설명된 민감도 수준에 따라 분류 및 처리되어야 합니다.
- 자산 관리 보안은 **자산 관리 정책 (MDY-IT-POL-02)**에 자세히 설명되어 있습니다.

3.3. 액세스 제어

자산 액세스는 조직에서 가장 민감한 프로세스 중 하나입니다. 리소스에 대한 적절한 액세스 권한을 유지하지 못하면 조직이 심각한 위험에 처할 수 있습니다.

monday.com의 액세스 권한은 알아야 할 사항 및 최소 권한 원칙에 따라 제공됩니다. 액세스 제어의 모든 보안 측면은 **액세스 제어 정책 (MDY-IT-POL-01)**에 자세히 설명되어 있습니다.

3.4. 암호화

monday.com은 내부 운영과 관련된 정보 외에도 고객을 대신하여 민감한 정보를 관리합니다. 전송 중(한 구성 요소에서 다른 구성 요소로 전송되는 동안) 및 저장 중인(저장된 경우) 이러한 데이터의 암호화는 매우 중요합니다. monday.com의 암호화 보안 제어는 **암호화 사용 정책 (MDY-IT-POL-04)**에 자세히 설명되어 있습니다.

3.5. 물리적 및 환경적 보안

물리적 및 환경적 보안 측면은 monday.com이 물리적 건물과 자산을 보호하기 위해 사용하는 조치를 나타냅니다. **물리적 및 환경적 보안 정책 (MDY-PHY-POL-01)**에 자세히 설명되어 있습니다.

3.6. 운영 보안

기존 시스템의 용량 관리 및 회사 내 신규 시스템 수용 프로세스는 회사 정책에 따라 진행되어야 합니다. 변경 사항을 잘 제어할 수 있도록 변경 관리 프로세스가 마련되어 있습니다. 자세한 내용은 회사의 **IT 변경 관리 절차 (MDY-IT-PRD-01)**를 참조하세요.

monday.com이 고객을 대신하여 처리하는 정보를 손실로부터 보호하기 위해 **백업 정책 (MDY-IT-POL-05)**에 설명된 대로 합의된 정책에 따라 정기적으로 백업을 실행하고 테스트해야 합니다.

3.7. 통신 보안

통신 보안은 전송 중인 정보(한 IT 엔터티에서 다른 IT 엔터티로 전송되는 정보)에 대한 무단 액세스 방지를 처리합니다.

통신 보안은 **물리적 및 환경적 보안 정책 (MDY-PHY-POL-01)**과 **암호화 사용 정책 (MDY-IT-POL-04)**에서 모두 다룹니다.

3.8. 공급망 보안

monday.com은 서비스의 특정 측면에 대해 제삼자 솔루션을 사용합니다. 이러한 제삼자 관계에는 클라우드 서비스 제공 업체, 아웃소싱 계약자, 원격 지원 등이 포함될 수 있습니다. 제삼자 솔루션을 구현할 때 제삼자가 monday.com의 위험 수준에 부정적인 영향을 미치지 않도록 특정 보안 조치를 취해야 합니다.

공급망 보안은 **제삼자 보안 정책 (MDY-IT-POL-06)**에서 다룹니다.

3.9. 정보 보안 사고 관리, 비즈니스 연속성 계획(BCP) 및 사고 복구 계획(DRP)

monday.com은 고객을 대신하여 처리하는 데이터의 기밀성, 가용성 및 무결성에 영향을 미칠 수 있는 사고를 방지하기 위해 상당한 노력을 기울입니다. 그럼에도 불구하고 사고의 위험을 완전히 완화하는 것은 불가능합니다. 정보 보안 사고의 경우 monday.com은 가능한 한 최단 시간 내에 사고를 감지하고 억제합니다. 정보 보안 사고 처리의 모든 측면은 **정보 보안 및 데이터 사고 대응 절차 (DOC-15)**와 **재해 복구 계획(DRP) (MDY-ORG-POL-03)** 및 **비즈니스 연속성 계획 (BCP) (MDY-BCP-PLN-01)**에서 다룹니다.

3.10. 제품 보안 및 보안 개발

monday.com의 서비스는 monday.com 고객을 대신하여 민감하고 중요한 데이터를 처리합니다. 따라서 서비스는 정보의 기밀성, 가용성 및 무결성을 보장하기 위해 최고 수준의 보안으로 개발되어야 합니다. monady.com의 보안 개발 관행 및 취약성 관리에 대한 자세한 내용은 **S-SDLC 정책 (MDY-DEV-POL-01)** 및 **패치 관리 정책 (MDY-DEV-POL-02)**을 참조하세요.

3.11. 규정 준수

monday.com은 관련 법률, 규정 및 표준을 준수하기 위해 최선을 다합니다. 이는 새로운 지역 및 국제 법률과 새로운 규정 및 새로운 표준 발표를 지속적으로 확인함으로써 이루어집니다.

4. 정책 수명 주기

4.1. 추가, 변경, 삭제

- 확립된 정책, 표준 및 기준선에 대한 변경은 필요에 따라 이루어져야 합니다.
- 각 변경 요청에는 그러한 변경을 요청하는 비즈니스 근거가 포함되어야 합니다.
- VP 운영팀은 각 요청을 검토하고 승인/거부해야 합니다.

- 보안팀은 관련된 모든 변경 사항이나 추가 사항을 회사 직원들에게 전달할 책임이 있습니다.

4.2. 검토 프로세스

- 글로벌 정보 보안 정책은 비즈니스 또는 규제 요구 사항에 따라 매년 또는 필요할 때 검토 및 업데이트되어야 합니다.
- 정보 보안 정책, 표준 및 기준선은 다음 사항을 일관되고 적절하게 처리하는지 확인하기 위해 최소 12개월마다 검토되어야 합니다:
    - 비즈니스 요구 사항 및 비즈니스 환경 – 제어는 비용 및 지속적인 운영 관점에서 모두 효과적이어야 하며 프로세스에 불합리한 중단을 일으키지 않고 비즈니스를 지원해야 합니다.
    - 외부 기술 환경 – 변화, 추세 및 새로운 개발로 인해 생성된 기회와 위협.
    - 내부 기술 환경 – 회사의 기술 사용으로 인한 강점과 약점.
    - 법적, 규제 및 계약 요구 사항.
    - 새롭거나 고유한 상황에 특정한 기타 요구 사항.

4.3. 책임 위임

- CISO는 필요에 따라 특정 직원이나 부서에 특정 역할과 책임을 위임할 수 있습니다.
- 위임된 책임은 양도할 수 없습니다.

4.4. 정책 예외

- 회사의 직원 및 제삼자는 상기 정책 및 표준을 준수해야 합니다.
- 정책이나 표준을 준수할 수 없는 경우 CISO는 이러한 기준에 대한 예외를 고려해야 합니다.
- 보안 포럼의 권장 사항에 따라 CISO가 결정한 대로 예외의 이점이 결과적인 위험보다 더 중요한 경우에만 예외가 허용될 수 있습니다.
- 예외를 적용 가능한 경우 합의된 개선 전략을 적시에 실행할 수 있도록 기한을 지정해야 합니다.
- 예외 사항을 정기적으로 검토하여 시정 조치가 제 시간에 이루어졌는지 확인해야 합니다.