# monday.com 보안 & 개인정보

monday.com

# 자주 묻는 질문에 대한 답변
## 필요한 답변을 얻을 수 있습니다

monday.com 보안 & 개인정보 FAQ에 오신 것을 환영합니다. 이 문서에서는 저희 애플리케이션 및 인프라 API, 인시던트 준비도 등에 대해 자주 묻는 질문에 대한 답변을 제공하고 있습니다. 이 문서에는 가장 빈번하게 나오는 질문에 대해서 답변을 드리고 있으니, 추가적인 질문이나 설명이 필요하신 분들은 언제든 지원팀 support@monday.com으로 연락주세요.

**목차**


기업 보안 ..... 1
애플리케이션 보안 ..... 4
인프라 보안 ..... 7
인시던트 준비 ..... 9
연동 옵션 ..... 9


## 기업 보안

1 **Q: monday.com에 공식적인 정보 보안 프로그램이 마련되어 있나요?**
**A:** 그렇습니다. 이 프로그램은 monday.com에 적용할 수 있는 로컬 및 국제 적용 법률, 표준 및 규정을 고려하고, monday.com 서비스와 고객의 데이터를 보호하기 위해 마련된 조치 및 제어를 정의합니다. 이 프로그램은 ISO 27001에 기반을 두고 있으며 자회사, 직원, 계약자, 하청업체, 파트너 및 monday.com을 작성, 유지보수, 저장, 액세스, 프로세스 또는 전송하는 모든 사용자를 포함한 monday.com 조직 전체를 포함합니다. monday.com에서 제공하는 서비스의 성능과 관련하여 해당 사용자의 정보를 확인할 수 있습니다.

**2** **Q: 현재 날짜 기준으로 어떤 보안 및 개인정보 관련 규정, 표준, 인증 등을 따르고 있나요?**

**A:** 다음과 같은 인증서, 보고서 및 준수 프로그램이 있습니다.

ISO 27001 ISO 27017 ISO 27018 ISO 27032

ISO 27701 SOC 1 Type II SOC 2 Type II SOC 3

HIPAA GDPR CCPA aws partner network CSA cloud security alliance®

여기에서 모든 인증서를 찾아보실 수 있습니다.

**3** **Q: monday.com에 보안 전담 직원이 있습니까?**

**A:** 네. 인프라, R&D, 운영 및 IT팀의 대표로 구성되어 있는 보안 팀과 더 넓은 보안 포럼이 존재합니다.

**4** **Q: 개인정보 보호정책/규정에 대한 업데이트 사항을 해결하기 위한 monday.com의 공식 프로세스가 있습니까?**

**A:** 법률 팀과 개인정보 보호 및 보안 팀의 대표와 DPO로 구성된 개인정보 보호정책 포럼은 적용 가능한 개인 정보 보호법/규정 및 규제 지침에 대한 업데이트를 지속적으로 모니터링합니다. 포럼은 "Privacy by Design" 접근법을 준수하고 정기적으로 데이터 보호와 관련하여 새로운 또는 제안된 제품 개발 및 기타 이니셔티브가 수반하는 영향을 평가합니다.

**5** **Q: monday.com은 PCI-DSS를 준수하고 있습니까?**

**A:** monday.com은 PCI-DSS 인증된 결제 서비스를 사용하므로, 제3자 청구 프로세서를 통해 지불되는 임의의 신용카드 결제는 PCI-DSS을 준수합니다. monday.com의

서비스 자체는 PCI-DSS에 따라 서비스에 대한 요금청구 정보를 처리하지 않으므로 PCI-DSS 데이터는 monday.com 내에 저장되지 않습니다.

**6** **Q: monday.com은 정보 보안 인증 프로그램을 보유하고 있습니까?**

**A:** 네. 저희 직원들은 초기 온보딩 과정의 일부로서 (적어도 매년) 각자의 정보 보안 의무에 관한 교육을 받고 있습니다.
또한 직원들의 정보 보호 의식을 높이기 위해 분기별로 보안 & 개인정보 보호 위크를 가지고 있습니다. 더불어 개발자들은 정기적으로 보안 트레이닝을 수행하여 보안 관련 개발 우수 사례를 최신 상태로 유지할 수 있습니다.

**7** **Q: monday.com은 얼마나 자주 정보 보안 정책을 검토합니까?**

**A:** 저희의 정보 보안 정책은 적어도 1년에 한 번 검토되며, 서비스나 보안 및 개인정보에 대한 변화에 따라 추가적으로 검토합니다.

**8** **Q: monday.com내의 개인정보 보호정책이 있습니까?**

**A:** 네, 여기에서 개인정보 보호정책을 찾을 수 있습니다.

**9** **Q: monday.com에서 공유하는 개인 데이터에 액세스할 수 있는 프로세서/서브 프로세서를 사용하고 있습니까?**

**A:** 네, 서비스 성능을 위해 몇 개의 서브 프로세서를 사용합니다. 제공하는 서비스 위치 및 타입을 포함한 서비스 프로세서(최종 사용자를 위한 데이터 처리)의 리스트는 여기서 확인할 수 있습니다.

위의 링크를 통해 서브 프로세서 목록의 변경사항에 대한 이메일 알림을 수신하도록 등록할 수도 있습니다.

# 애플리케이션 보안.

**10** **Q: monday.com은 어떤 유형의 데이터를 수집합니까?**

**A:** 새 계정을 작성할 때 제공되는 개인 정보를 저장합니다(사용자의 이름, 이메일 주소 및 전화번호). monday.com 서비스를 사용하기 시작하면 서비스 사용 및 데이터 유형(예: 텍스트, 파일 등) 에 따라 데이터가 저장되며 서비스에 로그인한 권한이 부여된 사용자가 monday.com로 제출하여 업로드하도록 결정합니다. 자세한 정보는 개인정보 보호 정책에서 찾을 수 있습니다.

**11** **Q: monday.com 서비스에 대한 사용자의 액세스를 어떻게 보호합니까?**

**A:** monday.com에 대한 액세스는 다음과 같은 인증 방식을 통해 수행됩니다.

- 크리덴셜: 사용자 이름(보통 이메일 주소) 및 암호
- Google SSO (Pro & Enterprise 플랜 전용) 및 Okta, OneLogin 및 사용자 정의 SAML 2.0과 같은 외부 ID 제공자 사용 지원(엔터프라이즈 플랜에만 해당).
- 또한, 문자 메시지 또는 인증자 애플리케이션을 통한 2단계 인증(2FA)은 계정 관리자에 의해 선택적으로 활성화될 수 있습니다.

**12** **Q: monday.com에서 비밀번호 정책을 지원합니까?**

**A:** 관리자는 두 가지 비밀번호 보안 설정을 선택할 수 있습니다. 반복 또는 연속 문자가 없는 최소 8자, 최소 하나의 숫자(123), 하나의 소문자(abc) 및 대문자(ABC)를 포함하는 8자 이상의 비밀번호를 사용할 수 있습니다.

**13** **Q: monday.com 고객의 데이터는 암호화되어 있습니까? 암호화를 위해 어떤 방법론을 사용하고 있습니까?**

**A:** 네, 있습니다. monday.com은 고객 데이터를 암호화하기 위해 다음과 같은 방법을 씁니다:

- 저장 데이터는 AES-256을 사용하여 암호화합니다.
- 전송 중인 데이터는 TLS 1.3 (최소 TLS 1.2)을 이용하여 암호화합니다.
- 사용자 비밀번호는 임의의 추가 값을 더하고 알고리즘화하여 암호화 됩니다.

**14** **Q: monday.com에서 코드가 안전하게 개발되고 있는지 어떻게 확인할 수 있습니까?**

**A:** OWASP Top 10과 CVSS 표준을 준수하여 소프트웨어 개발 라이프사이클에 대한 보안을 구축합니다. 개발자가 작성한 모든 코드는 정적으로 분석되고 피어 리뷰되어 배치 전에 코드 품질을 확인할 수 있습니다. 배치 시와 이후 취약점에 대한 애플리케이션을 지속적으로 평가하고 모니터링합니다.

**15** **Q: monday.com은 애플리케이션 보안 테스트를 실행합니까?**

**A:** 네, 애플리케이션 침입 테스트는 다양하고 독립적인 제3자가 매년 실행하고 있습니다. 추가적으로 버그 바운티 프로그램과 DAST 스캔은 최소 2주 단위로 수행됩니다.

**16** **Q: monday.com은 데이터를 얼마나 보관합니까? 서비스 사용을 중단하면 어떻게 되나요?**

**A:** 고객은 업로드된 자신의 데이터를 완전히 제어할 수 있고, monday.com을 사용하는 기간 동안에는 데이터를 수정하거나 삭제할 수 있습니다. (monday.com의 유저 인터페이스에서) monday.com 에서 수행하는 계정 종료 프로시저의 일부로 데이터 삭제를 요청할 수도 있습니다. (관리자 패널) 제출된 모든 데이터는 90일 이내에 삭제됩니다. 이 기간에는 롤백을 허용하는 30일 기간이 포함되며

데이터베이스 및 하위 프로세서의 데이터베이스에서 데이터를 삭제하는 추가 60일이 포함됩니다. 또는 계정을 중지하고 등록을 취소한 후에도 계정 데이터를 유지하도록 선택할 수 있습니다. 이 경우 현재 정책은 특정 지속 기간에 대한 약정 없이 유지하는 것입니다. 이 경우 통지 후 또는 통지 없이 삭제할 수 있습니다.
두 가지 형식으로 언제든지 계정에서 데이터를 내보낼 수 있습니다.

- 보드를 엑셀로 내보낼 수 있습니다
- 전체 계정의 데이터는 관리자 패널을 통해 Excel 시트 및 계정에 업로드된 파일을 포함하는 zip 아카이브로 내보낼 수 있습니다 (관리자에게만 한정됨).

**17** **Q: Q: monday.com에서 사용자 활동의 감사 로그를 플랫폼에 제공합니까?**
**A:** 네, 로그는 다음 두 가지 방식으로 제공됩니다

- 보드 수준 활동은 활동 로그에서 볼 수 있습니다
- 성공/실패 로그인 시도는 감사 로그에서 볼 수 있습니다

**18** **Q: monday.com 애플리케이션에서 사용할 수 있는 권한 부여 역할은 무엇인가요?**
**A:** 서비스 내의 역할에는 관리자, 멤버, 게스트, 뷰어가 있습니다. 여기서 자세한 내용을 볼 수 있습니다.
또한 서비스 내의 액세스 제어는 워크스페이스, 보드 유형, 보드 레벨 권한 및 컬럼 레벨 권한과 같은 기능을 활용하여 수행됩니다.

**19** **Q: 외부 업체에서 monday.com의 보안 취약점을 보고하기 위한 쉬운 방법이 있습니까?**
**A:** 예, 보안 취약점은 security@monday.com 으로 보고하거나 당사의 HackerOne 취약성 제출 양식을 통해 보고할 수 있습니다.

# 인프라 보안

**20 Q: monday.com의 데이터 센터는 어디에 있습니까?**

**A:** monday.com은 완전한 클라우드 서비스입니다. 당사의 서비스는 여러 가용성 영역에 걸쳐 서로 다른 지역에 구축된 DR 사이트를 사용하여 북부 버지니아주에 있는 Amazon Web Services 인프라에 호스트되어 있습니다. 특정 백업 데이터는 Google Cloud Platform (미국, 다중 영역) 에 저장됩니다. 이러한 데이터 센터는 선도적인 물리적 및 환경적 보안 조치를 채택하여 탄력적인 인프라를 구축합니다. 보안 사례에 대한 자세한 정보는 다음 사이트에서 확인할 수 있습니다.

AWS 보안 페이지

GCP 보안 페이지

**21 Q: monday.com 서비스를 온프레미스 버전으로도 이용할 수 있습니까?**

**A:** monday.com은 완전히 클라우드 기반 서비스이며 구축형 버전은 제공하지 않습니다.

**22 Q: 데이터는 얼마나 자주 백업합니까?**

**A:** 5분마다 사용자 데이터를 일관되게 백업하고 25일 동안 보유하고 있는 여러 AWS 가용성 영역에 암호화된 백업을 배포합니다. 또한 별도의 AWS 리전에 재난 복구 사이트를 설치했습니다. 활동 로그 데이터는 7일 동안 저장되는 GCP (미국, 다중 영역) 에 백업됩니다.

**23 Q: monday.com에 재난 복구 플랜이 있습니까?**

**A:** 네. 우리의 DRP는 생산 환경에 영향을 미치는 장애를 처리하고, 전용 DR 위치에서 서비스 핵심 기능을 복원하는 것을 포함합니다. 시험은 적어도 1년에 적어도 2회 수행됩니다.

**24 Q: monday.com은 물리적 보안 정책을 가지고 있습니까?**

**A:** Y네. 위에서 말했듯 당사의 서비스는 완전히 클라우드 기반이며, 그 어떤 인프라도 온프레미스가 아닙니다. 본사의 물리적 보안에는 개인 식별, 24/7 CCTV 감시 및 알람 시스템을 기반으로 한 액세스 제어가 포함되어 있습니다.

**25 Q: 서비스 가용성을 어떻게 보장합니까?**

**A:** W마이크로 서비스 아키텍처를 사용하여 하나 이상의 컴포넌트가 실패하는 경우 시스템 상태에 미치는 영향을 최소화할 수 있습니다. 다중 가용성 영역은 추가 중복성을 제공하는 데 사용되며 의존하는 일부 서비스에 대해 대체 제공자가 있습니다.
엔터프라이즈 고객에게는 SLA에 준하여 99.9% SLA가 제공됩니다. 또한 상태 페이지를 통해 서비스 가용성을 모니터할 수 있으며, 여기서 이메일 또는 텍스트 메시지를 통해 업데이트를 수신하도록 등록할 수도 있습니다.

**26 Q: monday.com 에서 보안 아키텍처 설계를 위한 우수 사례를 보유하고 있습니까?**

**A:** 예, 당사는 n AWS Advanced Technology Partner. 입니다. 이는 AWS 자체가 monday.com의 보안, 우수 사례 설계 등과 관련하여 엄격하게 조사해 왔다는 것을 증명합니다.

**27 Q: monday.com 에서 고객 데이터의 안전한 삭제를 지원합니까?**

**A:** 그렇습니다. 당사의 서비스는 AWS 에서 호스팅되며, 특정 데이터는 GCP로 백업됩니다. 두 클라우드 컴퓨팅 제공자 모두 다중 테넌트 환경에서 민감한 데이터를 안전하게 저장하고 삭제할 수 있도록 독점적인 데이터 분배 및 삭제 전략을 구현합니다. NIST (800-88) 에 상세히 설명된 기술들을 사용하여 상술한 제공자들에 의해 저장 매체 해체가 수행됩니다.

## 인시던트 준비

**28** **Q: monday.com에 공식적인 인시던트 응답 계획이 있습니까?**
**A:** 네. 당사의 인시던트 응답 계획은 인시던트를 발견하고 관련 인력, 커뮤니케이션 (내부 및 외부), 조사, 경감 및 사후 분석에 대해 이를 확대하기 위한 내부 지침을 제공합니다. 추가 정보는 DPA 통신에 대한 섹션 7 (데이터 인시던트 관리 및 알림) 에서 찾을 수 있습니다.

**29** **Q: monday.com이 사고나 위반으로 개인 데이터가 손상되었는지 여부를 확인하는 방법은 무엇입니까?**
**A:** 형식은 인시던트의 유형, 범위 및 스케일에 따라 다르지만, 최소한 계정 관리자에게 보내는 이메일을 포함합니다. 귀하는 침해의 성격, monday.com의 유해성, monday.com이 취한 조치와 취할 계획에 대해 자세히 알게 될 것입니다.

## 연동 옵션

**30** **Q: monday.com은 API 액세스를 제공합니까?**
**A:** 예, 여기에서 GraphQL API에 대한 문서를 찾을 수 있습니다.

**31** **Q: monday.com에서 서비스와 추가 통합을 지원합니까?**
**A:** 그렇습니다. 당사의 API외에도, Zoom , Slack, Zendesk, Microsoft Teams, Salesforce, Outlook 등을 포함하여 사용자 정의된 워크플로우를 작성하기 위해 필요한 다양한 기타 소프트웨어 솔루션과의 연동을 지원합니다. 이는 관리 패널에서 사용 안함으로 설정할 수 있는 선택적 기능입니다.