사용 제한 정책

2023 년 4 월

본 사용 제한 정책('**AUP**')은 사용자 및 사용자 대리인이 당사에서 제공하는 온라인 서비스('**클라우드 서비스**')를 이용할 때 준수해야 하는 약관을 규정합니다.

1. **자격 증명**
   사용자는 다음 사항을 준수합니다.
   - 클라우드 서비스에 대한 액세스 권한을 얻기 위해 거짓 신원을 사용하지 않습니다.
   - 액세스 자격 증명과 보안 토큰을 신중하게 저장하고 이를 무단으로 액세스하거나, 공개하거나 사용하지 않습니다.
   - 사용자 계정 또는 당사에서 허용하는 기타 수단 이외의 다른 수단으로 클라우드 서비스에 액세스하지 않습니다.
   - 사용자 계정, 기본 기술 또는 이와 관련된 호스트, 네트워크 또는 계정의 인증 또는 보안을 우회하거나 공개하지 않습니다.
   - 액세스 자격 증명을 다른 개인과 공유하지 않으며 자격 증명이 부여된 개인만 사용합니다. 당사는 합리적인 재량에 따라 변경이 필요하다고 판단하면 액세스 자격 증명을 변경할 수 있습니다.

2. **불법이거나 유해하거나 불쾌감을 주는 행위 또는 콘텐츠 금지**
   클라우드 서비스를 불법이거나 유해하거나 불쾌감을 주는 용도로, 또는 불법이거나 유해하거나 부정하거나 타인의 권리를 침해하거나 불쾌감을 주는 콘텐츠를 전송, 저장, 게시, 배포 또는 달리 제공 가능하도록 하기 위해 사용하거나 타인이 사용하도록 권장, 조장, 도모 또는 지시하지 않습니다. 클라우드 서비스 및 클라우드 서비스에 저장된 콘텐츠를 사용하여 다음과 같은 행위를 하지 않습니다.
   - 법이나 법규를 위반하거나 타인의 권리를 침해하는 행위
   - 부정한 제품, 서비스, 계획 또는 프로모션, 투자 사기, 다단계 또는 피라미드 사기, 피싱, 파밍 등을 제안하거나 유포하는 것을 포함하여 타인 또는 당사의 명성에 위해를 끼칠 수 있는 행위
   - 하이퍼링크를 입력, 저장 또는 전송하거나, 사용 권한이 없거나 불법인 콘텐츠 내부 또는 일부에 내장된 위젯 또는 기타 액세스 수단을 포함한 외부 웹사이트 또는 데이터 피드에 대한 액세스를 허용하는 행위
   - 타인의 명예를 훼손하거나, 외설적이거나, 폭력적이거나, 프라이버시를 침해하는 행위

3. **사용 제한 위반 금지**
   사용자는 다음 사항을 준수합니다.
   - 클라우드 서비스를 재판매, 양도, 재인가, 대여, 임대 또는 게시하거나 비즈니스 프로세스 아웃소싱, 기타 아웃소싱 또는 시간 공유 서비스 운영에 사용하지 않습니다(당사에서 명시적으로 허용하지 않는 한).
   - 클라우드 서비스 또는 기본 기술의 소스 코드를 리버스 엔지니어링, 분해, 디컴파일 또는 수정하거나, 이를 기반으로 한 파생물을 생성, 병합, 변조, 복구 또는 검색하려고 시도하지 않습니다(이러한 제한 사항이 관할권의 적용 가능한 법과 충돌하는 경우 제외).
   - 유럽 연합, 미국 및/또는 기타 해당 국가(들)의 적용 가능한 제재 및/또는 (재)수출 통제법과 규정에 따라 제재 또는 라이선스 요구사항에 의해 금지되거나 이러한 대상이 되는 지역에서 클라우드 서비스에 액세스하지 않으며, 적용 가능한 (재)수출 통제법 또는 해당 정부 라이선스 또는 승인에서 달리 허용하는 경우를 제외하고 통제되지 않는 콘텐츠(예: 분류는 EU 의 경우 'N', ECCN 의 경우 'N' 또는 미국의 경우 'EAR99')만 업로드합니다.

4. **악용 행위 금지**
   사용자는 다음 사항을 준수합니다.
   - 클라우드 서비스, 모니터링에 적용되는 사용 규제 및 제한사항(예: 액세스 및 저장 제한)을 피하거나 회피하거나 수수료 발생을 방지하기 위한 방식으로 클라우드 서비스를 사용하지 않습니다.
   - 성능 테스트를 수행하거나 경쟁 제품 또는 서비스를 구축하거나 기능 또는 사용자 인터페이스를 복제할 목적으로 클라우드 서비스에 액세스하거나 사용하지 않습니다.
   - 당사 시스템의 적절한 기능 또는 보안을 방해하지 않습니다.
   - 상업적인 광고 및 정보 안내 등 요청하지 않은 대량 이메일이나 기타 메시지, 프로모션, 광고 또는 권유 메일을 배포, 공개, 발송하거나 발송을 돕는 행위를 하지 않습니다. 메일 헤더를 변경하거나 숨기거나, 또는 발신자의 명시적인 허가 없이 발신자의 신원을 가장하지 않습니다.

5. **보안 침해 금지**
   클라우드 서비스 또는 기본 기술의 보안을 위협하거나 위협할 수 있는 방식으로 클라우드 서비스를 사용하지 않습니다. 사용자는 특히 다음 사항을 준수합니다.
   - 클라우드 서비스에 연결 및/또는 액세스하는 데 사용하는 시스템, 현장 하드웨어, 소프트웨어 또는 서비스에 대한 보안 공격, 바이러스 및 악성 코드에 대해 합리적인 예방 조치를 취합니다.
   - 당사의 명확한 사전 서면 동의 없이 클라우드 서비스 또는 기본 기술에 대한 침투 테스트를 수행하지 않습니다.
   - 산업 표준 보안 정책(예: 암호 보호, 바이러스 보호, 업데이트 및 패치 수준)을 준수하지 않는 클라우드 서비스에 액세스하거나 사용하기 위해 장치를 사용하지 않습니다.

6. **모니터링; 신고**
   사용자는 당사와 당사의 협력업체가 클라우드 서비스를 통해 사용자의 AUP 준수 여부를 모니터링할 수 있음을 인지합니다. 당사는 본 이용방침을 위반하는 행위를 조사할 수 있는 권리가 있습니다. 이러한 AUP 에 대한 위반을 알게 되는 경우 당사에 즉시 통지해야 하며, 당사가 요청한 대로 그러한 위반을 중지, 완화, 시정하는 데 필요한 지원을 제공해야 합니다. 당사는 본 AUP 또는 클라우드 서비스 사용에 대해 사용자와 체결한 기타 계약을 위반하는 콘텐츠 또는 리소스를 제거, 액세스 비활성화 또는 수정할 수 있습니다. 당사는 법률이나 규정 위반이 의심되는 행위를 관련 법률 집행기관, 규제 당국이나 기타 관련된 제 3 자에 신고할 수 있습니다. 제 3 자가 사용자의 클라우드 서비스 또는 사용자 콘텐츠 사용이 해당 제 3 자의 권리 또는 법률 또는 규정을 위반한다고 주장하는 경우 해당 고객 정보를 공유할 수 있습니다.

7. **Copyright / DMCA**. Siemens 는 저작권 정책에 따라 콘텐츠와 관련된 저작권 침해 통지에 대응하며, 이러한 정책은 관련 Siemens 계열사의 웹사이트 또는 사용자가 클라우드 서비스에 액세스하는 웹사이트에서 웹 링크를 통해 확인할 수 있습니다..