

---

# Cloud Software Group

## 서비스 보안 별첨

버전 3.0

2022년 9월 30일 발효

---

---

Cloud.com

---

## 목차

범위 .....	3
보안 프로그램 및 정책 기준.....	3
액세스 제어 .....	4
시스템 개발 및 유지 관리.....	5
자산 관리 .....	5
HR 보안 .....	6
운영 보안 .....	7
암호화 .....	8
물리적 보안 .....	8
비즈니스 연속성 및 재해 복구.....	9
인시던트 대응 .....	10
공급업체 관리 .....	10
규정 준수 .....	11
고객 감사 및 문의 .....	12

본 Cloud Software Group, Inc. (“Cloud Software Group”, “당사” 또는 “당사의”) 서비스 보안 별첨(“별첨”)은 관련된 Cloud Services Group 라이선스 및 또는 서비스 계약과 해당하는 서비스의 주문(총칭하여 “계약”)에 따라 고객(“고객”, “귀하” 또는 “귀하의”)에게 제공되는 클라우드 서비스, 기술 지원 서비스 또는 컨설팅 서비스(“서비스”)의 성능과 관련하여 구현된 보안 제어를 설명합니다. 서비스 제공과 관련되지 않은 베타 또는 랩/기술 미리 보기 서비스(Cloud Labs 포함)와 내부 IT 시스템은 본 별첨의 범위에 포함되지 않습니다.

굵게 표시된 용어는 계약에 명시된 의미 또는 여기에 정의된 의미를 가집니다. “고객 콘텐츠”는 당사가 서비스를 수행하기 위해 액세스 또는 수신하거나 저장 또는 처리를 위해 보내거나 업로드하는 모든 데이터를 말합니다. 또한 여기에는 시스템 또는 네트워크 구성 및 제어 등의 환경과 관련된 전매 기술 정보가 포함됩니다. “로그”는 당사의 제품이나 서비스 사용과 관련된 성능, 안정성, 사용량, 보안, 지원, 하드웨어, 소프트웨어, 서비스 또는 주변 장치에 대한 정보를 의미합니다.

## 1. 범위

이 별첨은 당사 서비스의 기밀성, 무결성 및 가용성을 유지하기 위해 사용하는 관리적, 물리적 및 기술적 보안 제어를 설명합니다. 이러한 제어는 당사의 운영 및 서비스 시스템과 환경에 적용됩니다. Cloud Software Group은 서비스 보안 프로그램에 대해 ISO/IEC 27002를 기준으로 사용하며 개별 서비스에 대한 업계 인증 및 평가를 획득했습니다. 자세한 정보는 당사의 트러스트 센터의 “개인 정보 보호 및 규정 준수” 섹션에서 확인할 수 있습니다.

당사는 보안 관행을 지속적으로 강화 및 개선하고 있으며, 따라서 여기에 설명된 규제를 수정할 권리를 가집니다. 모든 수정은 해당하는 서비스

---

기간의 보안 수준을 약화하지 않는다.

## 2. 보안 프로그램 및 정책 기준

Cloud Software Group에는 회사 전체에서 다양한 비즈니스 영역을 대표하는 경영진이 설정하고 승인한 보안 프로그램 및 정책 기준이 있습니다.

### 2.1 보안 위험 감독

CROC(Cyber Risk Oversight Committee)는 보안 위험 관리 활동을 통제합니다. CROC는 여러 기능을 담당하는 관리진 및 리더십으로 구성됩니다. 경영진 리더십 팀은 위원회 회원을 정기적으로 심사하여 비즈니스 및 운영 영역을 충분히 다루고 있는지 확인합니다.

CROC는 분기별 1회 이상의 회의를 통해 회사 운영 및 서비스 제공 인프라의 보안 위험을 평가하고 해결하기 위한 지침, 통찰력 및 방향을 제시합니다.

---

## 2.2 보안 위험 관리

Cloud Software Group은 당사의 제품 및 서비스와 인프라에 대한 잠재적 위험 요소를 식별하는 SRM(보안 위험 관리) 프로그램을 활용하고, 이러한 위험 요소에 연결된 위험의 중요성을 평가하며, 위험 완화 전력을 개발하고, 해당 제품 및 엔지니어링 팀과 함께 이러한 전략을 구현합니다.

## 2.3 정보 보안

Cloud Software Group에는 보안 감독 및 정책 전략, 규정 준수와 시행을 담당하는 CISO(최고 정보 보안 책임자)가 지정되어 있습니다. 보안 모니터링 및 대응 부문 이사는 조사, 억제 및 재구성을 포함한 인시던트 대응 프로세스를 책임집니다.

## 2.4 물리적 보안 및 환경적 보안

Cloud Software Group 보안 팀은 당사의 시설에 대한 물리적 액세스를 감독합니다.

# 3. 액세스 제어

당사는 회사 시스템, 자산, 데이터 및 시설 액세스를 위한 적절한 권한을 할당하고 유지하도록 설계된 액세스 제어 수단을 사용하여 잠재적 피해, 침해 또는 손실로부터 보호할 것을 요구합니다. 또한 최소 권한의 원칙 또는 역할 기반 보안에 따라 사용자의 액세스를 업무 기능 또는 역할을 수행하는 데 필요한 것으로만 제한합니다.

관리자는 충분한 직무 분리를 제공하는 역할을 설계하여 작업 및 권한을 여러 직원에게 분산함으로써 부정 행위 및 오류로부터 보호합니다.

## 3.1 새 계정, 역할 및 액세스 요청

Cloud Software Group에서는 회사 시스템 또는 데이터에 대한 액세스를 공식적으로 요구합니다. 각 액세스 요청에는 해당 사용자의 관리자가 사용자의 역할 및 액세스를 확인하기 위한 최소 승인 프로세스가 필요합니다. 액세스 관리자는 시스템 또는 데이터에 대한 액세스를 부여하기 전에 필요한 승인을 받았는지 확인합니다. 여기에는 최소 권한의 원칙이 적용됩니다.

## 3.2 계정 검토

당사는 사용자 계정 및 주요 시스템의 할당된 권한을 최소 연 2회 검토합니다. 검토의 결과로 변경이 필요할 경우 공식적인 액세스 요청 프로세스에 따라 사용자 및 사용자 역할에 해당 시스템에 대한 액세스가

---

필요한지 확인합니다.

### 3.3 계정, 역할 및 액세스 제거

당사는 사용자 역할의 변경(해당하는 경우), 종료, 사용자의 계약 종료 또는 퇴사를 통지받는 즉시 사용자 액세스를 비활성화, 해지 또는 제거할 것을 요구합니다.

액세스 제거 요청은 문서화되고 추적됩니다.

### 3.4 자격 증명

Cloud Software Group은 직원의 당사 시스템 원격 액세스에 대해 다단계 인증을 요구하며 다음과 같은 암호 처리 및 관리 관행을 시행합니다.

- 암호는 당사가 설정한 시스템 요구 사항에 설명된 대로 정기적으로 교체됩니다

- 암호는 숫자, 특수 문자, 대문자 및 소문자 조합, 최소 문자 수를 포함한 길이 및 복잡성 요구 사항을 충족해야 하며 일반 단어 또는 사전 단어를 허용하지 않아야 합니다
- 비활성화되거나 만료된 사용자 ID를 다른 개인에게 부여하지 않습니다
- 당사는 실수로 공개된 암호를 비활성화하는 절차를 고수합니다
- 당사는 유효하지 않은 암호를 사용하여 서비스에 액세스하려는 반복 시도를 모니터링하고 이러한 반복 시도를 차단하는 자동화된 조치를 취합니다

Cloud Software Group은 암호를 할당, 배포 및 저장할 때 다음과 같이 암호의 기밀성 및 무결성을 유지하도록 설계된 관행을 사용합니다.

- 암호 수명 주기에 걸쳐 암호를 해시 상태 및/또는 암호화 상태로 유지할 것
- 암호 공유를 금지할 것

## 4. 시스템 개발 및 유지 관리

당사는 계획된 보안 프로세스를 유지하며, 여기에는 정보 시스템의 보안 요구 사항을 해결하도록 설계된 표준 및 변경 제어 절차, 코드 검토 및 테스트와 테스트 데이터의 사용에 관한 보안이 포함됩니다. 이 프로세스는 전문 보안 팀에 의해 관리 및 모니터링되며 또한 설계 검토, 위협 모델링, 수동 코드 검토와 부분 확인 및 침투 테스트 작업도 담당합니다.

### 4.1 보안 설계 원칙

Cloud Software Group은 SDLC(공식 시스템 개발 수명 주기) 방법론을 채택하여 전산 정보 시스템 및 관련 기술 요구 사항의 개발, 취득, 구현 및 유지 관리를 통제합니다.

당사는 소프트웨어 기반 시스템을 사용하여 오픈 소스 검토 및 승인을 관리하며 여기에는 소프트웨어 제품의 주기적 검사 및 감사를 시행하는 것이 포함됩니다. 또한 오픈 소스의 사용과 오픈 소스 모범 사례에 대한 개발자 교육 및 관리에 관한 정책을 문서화하여 모든 직원에게 제공합니다.

### 4.2 변경 관리

당사의 인프라 및 소프트웨어 변경 관리 프로세스는 보안 요구 사항을 다루며 프로덕션 환경으로의 배포 전에 소프트웨어 및 인프라 변경의 권한 부여, 공식적 문서화, 테스트(해당하는 경우), 검토 및 승인을 요구합니다.

---

인프라 및 소프트웨어 변경은 작업 관리 시스템을 사용하여 관리 및 추적합니다.

변경 관리 프로세스는 적절히 분리되며 프로덕션으로 변경을 마이그레이션하기 위한 액세스 권한은 권한이 부여된 개인으로 제한됩니다.

## 5. 자산 관리

### 5.1 물리적 및 가상 자산 관리

Cloud Software Group은 서비스 수행을 위해 관리 및 사용하는 물리적 가상 시스템("서비스 자산")에 대한 동적 인벤토리를 유지합니다. 시스템 소유자는 당사의 보안 표준에 따라 해당하는 서비스 자산을 유지 관리하고 업데이트할 책임이 있습니다.

Cloud Software Group 및 고객 데이터는 공식적인 폐기 절차의 지침에 따라 안전하게 폐기됩니다. 당사는 분류에 따라 더 이상 필요하지 않은 데이터를 폐기하며, 이 때 데이터의 재구성 또는 판독을 방지하도록 설계된 삭제 프로세스를 사용합니다.

지정된 영역 또는 할당된 영역 안에서 더 이상 필요하지 않은 당사의 기술 자산은 식별 정보를 제거한 후 폐기됩니다. 기술 자산에는 개인 컴퓨팅 장치, 다기능 컴퓨팅 장치, 저장 장치, 이미지 처리 장치 및 네트워크 장비가 포함되며 여기에 국한되지 않습니다. 폐기 작업은 글로벌 보안 위험 서비스 및 정보 보안 팀을 통해 조정됩니다.

### 5.2 응용 프로그램 및 시스템 관리

응용 프로그램 및 시스템 소유자는 저장, 액세스, 폐기 또는 전송하는 데이터를 검토하고 분류할 책임이 있습니다. 다른 제어 중에서도 직원 및 계약업체는 다음을 수행해야 합니다.

- Citrix 기밀 정보의 최상위 2개 범주로 고객 콘텐츠를 분류하고 적절한 액세스 제한을 적용합니다
- 고객 콘텐츠의 인쇄를 제한하고 인쇄된 자료를 안전한 컨테이너에서 폐기합니다
- Citrix 보안 정책 및 표준의 요구 사항을 충족하지 않는 장비 또는 장치에 회사 정보 또는 기밀 정보를 저장하지 않습니다
- 컴퓨터 및 데이터에 자동으로 보안을 적용합니다.

### 5.3 데이터 보존

서비스 종료 이후 고객은 당사의 클라우드 서비스의 일부분으로 저장된 고객

---

콘텐츠에 제한된 시간 동안 액세스할 수 있습니다. 이 시간 이후 고객 콘텐츠는 고객에게 삭제를 알리는 확인 메시지를 전송한 후 삭제됩니다(백업 복사본 제외). 추가 세부 정보는 관련된 서비스 문서에 제공됩니다. 고객 콘텐츠는 서비스가 완료된 후 법적 용도로 필요할 경우에도 보존될 수 있습니다. Citrix는 이러한 고객 콘텐츠가 영구적으로 삭제될 때까지 이 별첨의 요구 사항을 준수합니다.

## 6. HR 보안

모든 직원 및 계약업체가 지켜야 할 핵심 요구 사항 중 하나는 고객 콘텐츠의 보안을 유지하는 것입니다. 모든 직원 및 계약업체는 당사의 비즈니스 행동 강령에 따라 보안 정책 및 표준을 준수해야 하며 특히 고객, 파트너, 공급업체 및 직원의 기밀 정보와 개인 정보를 보호해야 합니다.

모든 직원 및 계약업체에게는 고객 정보를 다루는 기밀 유지 계약이 적용됩니다. 또한 Cloud Software Group 보안 조직에서는 직원에게 정보 및 물리적 보안과 관련된 주제의 커뮤니케이션을 정기적으로 전파하여 특정 주제에 대한 보안 의식을 유지합니다.

### 6.1 신원 조회

당사는 현재 신원 조회 공급업체를 통해 전 세계의 모든 신규 고용을 조사하며 현지 법률 또는 고용 규제에 의해 제한되는 경우를 제외하고 타사 공급업체 직원에게도 동일한 조사를 요구합니다.

### 6.2 교육

모든 직원은 고객, 파트너, 공급업체 및 직원의 기밀 정보를 포함하는 당사의 기밀 정보에 대한 보안을 유지하도록 설계된 데이터 보호 및 회사 정책에 관한 교육을 받아야 합니다. 해당 교육에서는 개인 정보의 사용, 액세스, 공유 및 보존에 대한 제한 필요성과 같이 직원이 개인 정보를 처리할 때 적용되는 개인 정보 보호 관행 및 원칙을 다룹니다. 엔지니어링 조직의 구성원은 보안 개발, 아키텍처 및 코드 작성으로 구성되는 개별 교육을 받습니다.

### 6.3 시행

모든 직원은 당사의 보안 및 개인 정보 보호 정책과 표준을 준수해야 합니다. 이를 준수하지 않을 경우 최대 고용 종료의 처벌 조치가 내려집니다.

## 7. 운영 보안

### 7.1 네트워크 및 시스템 보안

---

Cloud Software Group에는 네트워크 및 시스템이 안전하게 구성되었는지 확인하도록 설계된 네트워크 및 시스템 강화 표준이 문서화되어 있습니다. 이러한 표준에서 요구되는 절차에는 다음을 포함되며 이에 국한되지 않습니다.

- 기본 설정 및/또는 계정 변경 또는 비활성화
- 관리 액세스의 사용 제어
- 서비스 계정에 대해 당시 생성된 용도로만 제한
- 감사에 적절한 로깅 및 알림 설정 구성

당사는 서버 및 워크스테이션에 멀웨어 차단 소프트웨어를 구현할 것을 요구하고 네트워크에서 악성 소프트웨어를 검사합니다.

네트워크 제어를 통해 고객 콘텐츠에 대한 액세스를 규제합니다. 네트워크 제어는 고객 콘텐츠에 대한 액세스를 통제합니다. 여기에는 해당하는 경우 다음이 포함됩니다. 인터넷과 내부 네트워크 간에 액세스 및 무단 트래픽을 제한하는 보안 메커니즘이 포함된 신뢰하지 않는 중간 영역 구성. 네트워크 분리를 통해 고객 콘텐츠의 무단 액세스 차단. 계층 간 트래픽을 제한하는 계층 구조를 사용하여 웹 및 응용 프로그램 서버를 해당하는 데이터베이스 서버에서 분리.

## 7.2 로깅

당사는 서비스가 올바르게 작동하는지 확인하고, 시스템 문제 해결을 지원하고, 네트워크 및 고객 콘텐츠를 보호하기 위해 로그를 수집합니다. 로그에는 액세스 ID, 시간, 부여되거나 거부된 권한, 진단 데이터(예: 추적 및 충돌 파일) 및 기타 관련 정보 및 활동이 포함됩니다.

당사는 (i) 서비스의 제공, 보안, 관리, 측정 및 개선을 위해, (ii) 고객 또는 고객의 최종 사용자의 요청에 따라, (iii) 청구, 계정 관리, 내부 보고 및 제품 전략을 위해 (iv) 계약, 정책, 관련 법률, 규정 또는 정부 요청을 준수하기 위해 로그를 수집하고 사용합니다. 여기에는 서비스 및 관련 구성 요소의 성능, 안정성, 사용량 및 보안에 대한 모니터링이 포함됩니다. 로그에는 액세스 ID, 시간, 부여되거나 거부된 권한, 진단 데이터(예: 추적 및 충돌 파일) 및 기타 관련 정보 및 활동이 포함됩니다. 고객은 이 모니터링을 차단하거나 간섭할 수 없습니다.

고객 콘텐츠 및 로그 취급에 대한 자세한 내용은 Citrix 클라우드 서비스 로깅에 대한 다양한 백서가 있는 당사의 트러스트 센터 [Cloud Assurance Data Protection & Security section](#)를 참조하십시오.

## 7.3 인증, 자격 증명 및 보안 관리

---

Cloud Software Group에서는 보호, 가용성 및 기밀성을 보장하기 위해 인증서, 자격 증명 및 기밀에 대한 수명 주기를 다루는 정책을 유지합니다. 기밀 관리자는 반드시 문서화되어야 하며 기밀 관리 직원으로서 책임을 다한다는 것을 공식적으로 인정해야 합니다.

책임에는 다음이 포함되며 이에 국한되지 않습니다.

- 인증서는 승인된 인증 기관에서 발급해야 합니다
- 암호화 키는 일반 텍스트로 저장하거나 전송할 수 없으며 공인된 강력한 암호화 프로토콜을 사용해야 합니다
- 자격 증명 및 암호는 매년 한 번 이상 교체해야 하며 공인된 권한 인증 관리 도구에 저장해야 합니다

#### 7.4 취약점 관리

당사는 응용 프로그램 및 시스템에서 자동화된 취약성과 포트 검색을 통해 취약점을 정기적으로 모니터링합니다.

확인된 취약성은 심각도 등급 및 공급업체 권장 사항에 따라 달라지는 타임라인에서 수정해야 합니다. 패치, 업데이트 또는 영구적 완화를 사용할 수 없는 경우 적절한 대응 조치를 통해 취약성에 대한 악용 위험을 줄입니다.

## 8. 암호화

### 8.1 전송 중 데이터의 보호

Cloud Software Group은 서비스의 일부인 공용 네트워크를 통한 정보 전송을 위해 보안 전송 프로토콜을 배포했습니다. 서비스는 암호화로 보호되며 인터넷을 통한 액세스는 TLS 연결로 보호됩니다.

### 8.2 유희 상태의 데이터 보호

당사는 서비스를 제공하는 데 사용되는 모든 워크스테이션에 최소 128비트 전체 디스크 암호화로 암호화를 요구합니다. 암호화되지 않은 고객 콘텐츠는 휴대용 장치에 저장할 수 없습니다.

일부 클라우드 서비스는 기본적으로 특정 데이터 요소를 암호화하며 고객이 구현할 수 있도록 다른 암호화 기능을 제공할 수도 있습니다. 자세한 내용은 해당되는 클라우드 서비스 문서를 참조하십시오.

## 9. 물리적 보안

### 9.1 시설

당사는 모든 시설에 대한 무단 액세스를 방지하도록 설계된 다음과 같은 제어를 유지합니다.

- 시설 액세스는 권한이 있는 개인으로 제한됩니다
- 방문자는 디지털 방문자 로그에 등록해야 하며 항상 인솔자가 따르거나 모니터링됩니다
- 직원, 계약업체 및 손님은 ID 배지를 가지고 있어야 하며, 시설에 있는 동안 항상 이 배지를 보여야 합니다
- 보안 팀에서는 시설에 대한 업무 시간 외 액세스를 관리하고 제어합니다
- 건물 진입 지점, 적재 및 적하 구역과 공공 구역은 보안 요원, 침입 탐지 및/또는 CCTV 카메라로 모니터링됩니다(접근 모니터링에 대한 메커니즘은 시설 및 위치에 따라 시설별로 다를 수 있음)

또한 Cloud Software Group 시설에서는 다음과 같은 기능을 제공합니다.

- 화재 진압 및 화재 탐지 시스템 또는 장치
- 실내 온도 조절 시스템 또는 장치(온도, 습도 등)
- 접근 가능한 수원 차단 또는 격리 밸브
- 비상구 및 대피 경로

사무실에 위치한 데이터 보관함은 배지 액세스를 통해 보호됩니다.

## 9.2 데이터 센터

위에 설명된 시설 제어에 더해 Cloud Software Group이 소유하고 관리하는 시설의 경우 서비스 제공에 사용되는 데이터 센터에 추가 제어가 구현됩니다.

당사는 정전 또는 회선 간섭으로 인한 데이터 손실을 방지하도록 설계된 시스템을 사용합니다. 여기에는 재해 복구 사이트에 설정된 글로벌 이중화 서비스 인프라가 포함됩니다. 데이터 센터 및 ISP(인터넷 서비스 공급자)를 평가하여 대역폭, 지연 시간 및 재해 복구 격리와 관련된 성능을 최적화합니다.

데이터 센터는 ISP 통신사에 독립적이고 물리적 보안, 이중화된 전원, 인프라 이중화 및 주요 공급업체의 작동 시간 계약을 제공하는 시설에 배치됩니다.

타사 데이터 센터 또는 클라우드 서비스를 사용하여 서비스를 제공하는 경우 당사 해당 시설의 물리적 및 환경적 보안 요구 사항 이상을 충족하는 공급자와 계약을 맺습니다.

---

## 10. 비즈니스 연속성 및 재해 복구

### 10.1 비즈니스 연속성

Cloud Software Group은 불리한 상황 또는 중단을 일으키는 상황 중의 비즈니스 운영 연속성을 전략적으로 계획하며 이러한 이벤트의 발생 중에 서비스 운영을 유지하는 시스템을 설계합니다.

당사는 부서 수준의 BIA(비즈니스 영향 분석)를 연 2회 이상 수행하며 매년 1회 검토합니다. BIA는 각 부서의 리소스 요구 사항, 복구 매개 변수 및 방법, 재배치 요구 사항 및 프로세스 전반에서 장애 또는 공백을 방지하는 데 필요한 보안 장치를 식별하고 문서화하는 부서별 BCP(비즈니스 연속성 계획)를 작성하는 데 사용됩니다. 각 부서의 관리직은 매년 또는 중요한 조직적 변경이 발생할 때 BCP를 검토하고 승인합니다.

당사 모든 시설에 대한 긴급 및 비상 계획을 유지합니다. 시설을 사용할 수 없게 될 경우 직원은 다른 Cloud Software Group 시설 또는 선택한 위치에서 원격으로 근무할 수 있습니다. 추가 복구 전략은 해당하는 경우 BCP에 문서화되어 있습니다.

### 10.2 재해 복구

당사는 서비스 또는 운영 중단의 영향을 최소화하기 위해 비즈니스 시스템 및 데이터의 안정적이고 질서 있는 복원 및 복구를 보장하도록 설계된 프로세스 및 제어를 구현합니다. Cloud Software Group은 모든 미션 크리티컬 시스템, 데이터 및 인프라에 이중화를 구현합니다. DRP(재해 복구 계획)에서는 위에 언급된 BIA에서 수행되는 평가를 사용하여 복구 시간 매개 변수, 방법, 우선 순위 및 프로세스 전반에서 장애 또는 공백을 방지하는 데 필요한 보안 장치를 식별하고 문서화합니다.

이 계획은 다음을 포함하되 이에 국한되지 않는 중요한 시스템 및 데이터의 복원을 위한 전체 구조 및 접근 방식을 개괄적으로 명시합니다.

- 개인 또는 팀의 역할 및 책임
- 필수 인력 또는 타사의 연락처 정보
- 필수 인력에 대한 교육 요구 사항 및 계획
- 복구 목표, 복원 우선 순위 및 성공 메트릭
- 전체 복구 및 복원의 스키마

관리직은 매년 또는 중요한 조직적 변경이 발생할 때 DRP를 검토하고

---

승인합니다.

## 11. 인시던트 대응

Cloud Software Group는 관리형 네트워크 및/또는 시스템 또는 고객 콘텐츠에 영향을 미치는 보안 인시던트에 대한 탐지, 보고, 식별, 분석 및 대응 프로세스를 상세히 다루는 사이버 보안 인시던트 대응 계획을 유지합니다. 보안 인시던트 대응 교육 및 테스트는 연 1회 이상 수행됩니다.

“보안 인시던트”는 기밀성, 무결성 또는 가용성 손실로 이어지는 고객 콘텐츠 무단 액세스를 의미합니다. 당사의 제어 범위 내의 고객 콘텐츠에 보안 인시던트가 발생했다고 판단되는 경우 당사는 법적으로 요구되는 기간 내에 고객에게 이를 알립니다. 당사의 고지에는 알려진 경우 인시던트의 본질, 기간 및 귀하에게 미치는 잠재적 영향이 설명됩니다. 당사는 각 보안 인시던트의 레코드를 유지합니다.

## 12. 공급업체 관리

Cloud Software Group은 하청업체 및 대행업체를 통해 서비스를 수행할 수 있습니다. 모든 하청업체와 대행업체는 서비스 수행에 필요한 대로만 고객 콘텐츠에 액세스할 수 있으며 해당하는 경우 이 별첨에서 당사에 요구하는 것 이상의 데이터 보안 수준을 제공할 것을 요구하는 서면 계약의 적용을 받습니다. 하청업체 및 대행업체가 계약의 해당 약관을 준수하는지 확인할 책임은 항상 당사에 있습니다. 고객 콘텐츠에 액세스할 수 있는 Cloud Software Group 하청 처리업체의 목록은 [트러스트 센터](#)에서 확인할 수 있습니다.

### 12.1 온보딩

당사의 타사 위험 관리 프로그램은 타사 공급업체의 사용에 의한 보안 위험의 관리를 위한 체계적인 접근 방식을 제공합니다. 또한 이러한 타사의 조달에 연계하기 전에 보안 위험을 식별, 분석 및 완화합니다.

Cloud Software Group은 공급업체와의 계약을 시행하여 이 별첨에 명시된 내용에 따라 관련된 보안 수단 및 의무를 문서화합니다.

### 12.2 지속적인 평가

당사는 공급업체 관계 전체에 걸쳐 보안 수단이 유지되는지 확인하도록 설계된 주기적인 보안 위험 평가를 수행합니다. 제공된 서비스의 변경 또는 기존 계약의 변경 시 이러한 변경이 추가 위험 또는 과도한 위험을 나타내지

---

않는지 확인하는 보안 위험 평가가 필요합니다.

### 12.3 오프보딩

당사는 공급업체 관계를 종료하거나 공급업체의 계약이 만료되기 최소 90일 전에 회사의 조달 조직에 통지하기 위해 노력합니다(조기 종료에 필요한 경우 제외). 회사의 조달 조직에서는 기존 관계의 종료를 조정하여 회사 데이터 및 자산이 안전하고 올바르게 처리되는지 확인해야 합니다.

## 13. 규정 준수

### 13.1 개인 데이터의 처리

개인 데이터는 식별되거나 식별 가능한 개인과 관련된 정보입니다. 귀하는 고객 콘텐츠에 포함할 개인 데이터를 결정합니다. 당사는 서비스 수행에 있어서 데이터 처리자 역할을 하며 귀하는 고객 콘텐츠에 포함된 모든 개인 데이터의 데이터 제어자 역할을 유지합니다. 당사는 계약에 명시된 대로 이러한 개인 데이터의 처리와 관련하여 귀하의 지시에 따라 행동합니다.

이러한 데이터의 해외 전송에 사용되는 메커니즘을 포함하여 GDPR(General Data Protection Regulation)이 적용되는 개인 데이터의 처리에 관한 추가 정보는 Cloud Software Group [데이터 처리 부칙](#)에 제공되어 있습니다.

### 13.2 서비스의 위치

클라우드 서비스 고객은 클라우드 서비스의 위치를 선택할 수 있습니다. 당사는 해당하는 클라우드 서비스 구독 중에 귀하가 선택한 환경의 지리적 위치를 동의 없이 변경하지 않습니다. 일부 클라우드 서비스는 특정 위치를 선택할 수 없으며, 일반 서비스 제공의 일부로 서비스 제공에 필요할 경우 고객 콘텐츠는 Citrix 및/또는 해당 서비스 공급자가 운영하는 미국 또는 기타 국가로 전송될 수 있습니다.

### 13.3 고객 콘텐츠의 공개

당사는 소환, 사법 또는 행정 명령 또는 기타 구속 법률 문서(각각 "요구")에 응하는 것을 포함하여 법적으로 요구되는 범위까지 고객 콘텐츠를 공개할 수 있습니다. 법률이 금하는 경우를 제외하고 당사는 즉시 귀하에게 모든 요구를 알리고 고객이 적시에 요구에 응하는 데 필요한 합당한 고객 지원을 제공합니다.

### 13.4 고객 보안 및 규제 요건

서비스는 고객의 대규모 IT 환경 안에서 제공되도록 설계되었으므로 Citrix를 통해 명시적으로 관리되지 않는 보안의 모든 측면, 즉 서비스와 함께 고객이 사용할 수 있는 서비스와의 기술적 통합, 사용자 액세스 관리 및 제어, 모든 응용 프로그램 및 네트워크를 포함하되 이에 국한되지 않는 모든 측면에 대한 책임은 전적으로 고객에게 있습니다.

귀하는 서비스의 일부로 고객 콘텐츠에 대한 액세스를 당사에 제공하는 것을 포함한 서비스 사용에 본 계약 조항 이외의 규제 또는 보안 요구 사항이 적용되는지 여부를 확인할 책임이 있습니다. 따라서 고객은 이 별첨에 포함되지 않은 특정 제어를 시행하는 법률에 의거하여 통제되는 고객 콘텐츠를 제출하거나 저장하지 않아야 합니다. 여기에는 계약 및 해당하는 서비스 설명에 명시된 경우와 당사에서 이러한 데이터를 처리하는 데 필요한 추가 계약(예: HIPAA Business Associate Agreement)을 타사가 사전에 체결한 경우를 제외하고, 미국 ITAR(International Traffic in Arms Regulations) 또는 방산 물자 또는 방산 서비스의 수출입을 제한하는 모든 국가의 유사 규정, PHI(Protected Health Information), PCI(Payment Card Information) 또는 정부 규정에 따라 배포가 제어되는 데이터가 포함될 수 있습니다.

### 14. 고객 감사 및 문의

Cloud Software Group은 최대 연 1회 고객 위험 평가에 대한 응답의 형태로 감사 요청에 응합니다. 또한 고객은 언제든지 당사의 Due Diligence 패키지에 액세스하여 업데이트된 보안 패키지 및 질문서를 받을 수 있습니다. 당사의 Due Diligence 패키지는 고객 보안 문의를 위해 작성되었으며 당사의 클라우드 서비스에 대해 완료된 Shared Assessments의 SIG(Standardized Information Gathering) Lite 질문서를 포함하여 쉽게 이용할 수 있는 보안 정보를 제공합니다. Due Diligence 패키지는 [클라우드 보증 데이터 보호 및 보안 섹션의 트러스트 센터](#)에서 다운로드할 수 있습니다.

### 15. 연락처

기능	연락처
고객 지원	<a href="https://www.citrix.com/contact/technical-support.html">https://www.citrix.com/contact/technical-support.html</a>
보안 인시던트 보고	의심되는 취약성
당사 서비스의	

#### 기업 영업부

북미 | 800-424-8749 (전

세계 동일) | +1 408-790-  
8000

#### 위치

본사 | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States Silicon Valley  
| 4988 Great America Parkway Santa Clara, CA 95054, United States

©2022 Cloud Software Group, Inc. All rights reserved. 여기에 표시된 모든 상표는 Cloud Software Group, Inc. 및/또는 해당 회사의 자산이며 미국 특허 및 상표국과 기타 국가에서 등록된 것일 수 있습니다. 기타 모든 상표는 해당 소유자의 재산입니다.