최종 수정 날짜: 2018년 3월 1일

Citrix 서비스 보안 별첨

본 Citrix 서비스 보안 별첨("별첨")은 Citrix 라이센스, 구독 또는 서비스 계약에 따라 Citrix Cloud Services, 기술 지원 서비스 또는 컨설팅 서비스와 관련하여 사용되는 기술 및 조직적 보안 제어를 설명한다. 이 별첨은 이러한 서비스 계약("계약")에 참조로 포함되어 있다. 이 별첨은 Citrix Cloud Labs를 비롯한 베타 또는 Lab/Tech Preview 서비스에는 적용되지 않는다.
주요 용어의 의미는 계약에 명시되어 있거나 아래의 7조(정의)를 포함하여 본 문서에 정의되어 있다.

1조. Citrix 보안 제어

이 조항은 Citrix가 서비스와 고객의 연결된 보안 의무를 보호하기 위해 사용하는 물리적, 논리적 및 관리상의 제어를 설명한다. Citrix는 ISO/IEC 27002를 서비스 보안 프로그램의 기준으로 사용한다.

모든 서비스에는 1.A절에 명시된 제어가 적용된다. 일반적으로 제공되는 모든 Citrix Cloud Services(통칭하여 "클라우드 서비스")에는 1.B절에 명시된 추가 제어가 적용된다.

Citrix는 고객이 지불한 서비스 기간 중에 적용되는 제어가 본 1조에 명시된 고객 콘텐츠를 해당 유효 날짜까지 보호하는 것을 조건으로 본 1조에 명시된 제어를 수정할 수 있는 권리를 보유한다.

1.A. 엔터프라이즈 보안 제어 - 모든 서비스

영역	제어
보안 프로그램 관리	**보안 소유권.** Citrix 에는 서비스의 보안 제어를 조정하고 모니터링하는 한 명 이상의 보안 책임자가 지정되어 있다. **보안 역할 및 책임.** 고객 콘텐츠에 액세스할 수 있는 Citrix 담당자는 기밀 유지 의무를 준수해야 한다. **서비스 보안 정책.** Citrix 는 Citrix 경영진에 의해 설정되고 승인되는 중요한 보안 및 안전 원칙을 제공하는 포괄적인 GSF(글로벌 보안 프레임워크)를 유지한다. 정책은 보안 요구 사항을 명확하고 간결하게 제공한다. 표준은 정책 요구 사항을 충족하기 위한 프로세스 또는 방법론을 정의한다. GSF 보안 프로그램은 정기적인 검토 및 평가를 받는다. Citrix 는 GSF 프로그램의 요약본을 유지하며 고객이 요청할 경우 제공한다. **제품 위험 관리.** Citrix 는 예를 들어 개인 정보 보호 위험 평가, 오픈 소스 검토 및

영역	제어
	내보내기 제어 분석 등 서비스와 관련된 위험의 주요 영역에 대한 평가를 수행한다.
자산 관리	**자산 인벤토리.** Citrix 는 서비스 수행에 사용되는 Citrix 관리 장비("자산")의 인벤토리를 유지한다. 인벤토리는 확인된 시스템 소유자를 통해 필요에 따라 유지되고 업데이트된다. **자산 및 데이터 처리** Citrix 는 고객 콘텐츠에 대한 액세스를 적절히 제한하기 위해 이러한 고객 콘텐츠를 식별하고 분류한다. Citrix 는 고객 콘텐츠의 인쇄 및 고객 콘텐츠가 포함된 인쇄된 자료의 배포를 제한한다. Citrix 담당자는 고객 콘텐츠를 휴대용 장치에 저장하거나, 고객 콘텐츠에 원격으로 액세스하거나, Citrix 또는 해당 서비스 공급자가 관리하는 설비 밖에서 고객 콘텐츠를 처리하기 전에 승인을 받아야 한다.
액세스 관리	**액세스 정책.** Citrix 는 고객 콘텐츠에 액세스하는 개인의 보안 권한에 대한 기록을 유지하고 최소 권한의 원칙을 준수한다. **액세스 권한 부여** Citrix 는 고객 콘텐츠가 포함된 Citrix 시스템에 대한 액세스 권한을 부여받은 개인의 기록을 유지하고 업데이트한다. 시스템에 대한 새로운 액세스 권한은 관리 팀의 검토 및 승인을 거친 후 부여된다. Citrix 는 주요 시스템에 대한 사용자 계정과 할당된 권한을 주기적으로 검토한다. Citrix 는 데이터 및 리소스에 대한 액세스 권한을 부여하거나 변경하거나 취소할 수 있는 담당자를 확보한다. Citrix 는 고객 콘텐츠가 포함된 시스템에 액세스할 수 있는 개인이 두 명 이상인 경우 각 개인이 구분된 식별자/로그인을 사용하도록 한다. **최소 권한** Citrix 는 고객 콘텐츠에 대한 액세스 권한을 업무 수행을 위해 고객 콘텐츠에 액세스해야 하는 개인으로 제한한다.

영역	제어
	무결성 및 기밀성 사용자는 자리를 비우는 동안 컴퓨터와 데이터를 보호할 의무가 있다. 암호는 암호의 수명 주기 전체에 걸쳐 알 수 없는 상태로 유지되어야 한다. **인증** Citrix 는 업계 표준 방식을 사용하여 정보 시스템에 액세스하는 사용자를 식별하고 인증한다. 인증 메커니즘이 암호에 기반하는 경우 Citrix 는 다음과 같은 업계 표준의 암호 처리 및 관리 방식을 따른다. 암호는 시스템 요구 사항 및 Citrix 표준에 설명된 바와 같이 주기적으로 갱신된다. 암호는 길이 및 복잡성 요구 사항(예: 최소 길이 8 자)을 충족해야 한다. 담당자는 암호를 공유할 수 없다. 비활성화되거나 만료된 식별자는 다른 개인에게 부여되지 않는다. Citrix 는 손상되거나 부주의로 공개된 암호를 비활성화하는 절차를 유지한다. Citrix 는 잘못된 암호를 사용하여 서비스에 액세스하려는 반복적인 시도를 모니터링한다. Citrix 는 암호의 기밀성 및 무결성을 유지하도록 설계된 방식을 사용하여 암호를 할당하고 배포하고 저장한다.
손실 방지	**악성 소프트웨어.** Citrix 는 공용 네트워크에서 시작된 악성 소프트웨어와 같은 악성 소프트웨어가 고객 콘텐츠에 무단 액세스할 수 없도록 바이러스 백신 소프트웨어 및 기타 제어를 사용한다. **미디어 폐기.** Citrix 는 더 이상 필요하지 않은 미디어를 분류에 따라 안전한 삭제 프로세스를 사용하여 폐기한다.

영역	제어
물리적 보안 및 환경적 보안(액세스 제어, 가용성 제어)	**Citrix 시설에 대한 물리적 액세스.** Citrix 시설에는 권한이 부여된 개인만 액세스할 수 있다. 시설 내의 직원, 계약직 근무자 및 방문객은 항상 ID 배지를 착용해야 하며 이러한 배지는 눈에 보이는 위치에 있어야 한다. Citrix 는 보안 요원, 침입 탐지 및 CCTV 카메라를 비롯한 다양한 방법을 사용하여 시설 진입 지점을 모니터링한다. **중단 시 손실 방지.** Citrix 는 전원 공급 장애 또는 회선 간섭으로 인한 데이터 손실을 방지하는 시스템을 사용한다. 여기에는 재해 복구 사이트가 설정된 글로벌 및 이중화 서비스 인프라, 대역폭, 대기 시간 및 재해 복구 격리 관련 성능 최적화를 위한 데이터 센터 및 ISP(인터넷 서비스 공급자) 평가, 물리적 보안, 이중화된 전원 및 인프라 이중화를 제공하는 ISP 통신 회사 중립적인 안전한 시설에 데이터 센터 배치 및 주요 공급업체의 작동 시간 계약이 포함된다. **호스트되는 데이터 센터.** Citrix 가 타사에 배치된 데이터 센터를 사용하여 서비스를 제공하는 경우 Citrix 는 해당 서비스 공급자에 Citrix 관리 시설의 물리적 및 환경적 보안 요구 사항 이상을 충족할 것을 요구한다. 최소 보안 요구 사항에는 다음이 포함되며 이에 국한되지 않는다. • 물리적 액세스 제한 및 보호(인증, 로그, 모니터링 등) • 적절한 환경 분리 • 화재 진압, 감지 및 예방 메커니즘 • 온도 조절 시스템(온도, 습도 등) **클라우드 컴퓨팅.** Citrix 가 XaaS[IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)]를 사용하여 서비스를 제공하는 경우 Citrix 는 호스트되는 데이터 센터와 거의 동일한 수준의 물리적 액세스 제어를 제공하는 XaaS 공급자와 계약한다.
응용 프로그램 및 개발 보안	**시스템 개발 및 유지 관리.** Citrix 는 정보 시스템의 보안 요구 사항, 코드 검토 및 테스트와 테스트 데이터의 사용에 관한 보안을 해결하도록 설계된 표준 및 변경 제어 절차를 포함하는 Secure by Design(보안 설계) 프로세스를 유지한다. 이 프로세스는 전문적인 보안 엔지니어링 팀에 의해 관리되고 모니터링된다. 이 팀은 설계 검토, 위협 모델링, 수동 코드 검토 및 임의 추출 검사와 침투 테스트도 수행한다. **오픈 소스 관리.** Citrix 는 소프트웨어 기반 시스템을 사용하여 오픈 소스 검토 및

영역	제어
	승인을 관리한다. 또한 Citrix 는 소프트웨어 제품의 주기적인 검사 및 감사를 시행하여 오픈 소스 규정 준수를 확인한다. **변경 관리.** Citrix 는 정보 시스템의 보안 요구 사항, 테스트, 테스트 승인 및 테스트 데이터 사용에 관한 보안을 해결하는 변경 제어 절차를 유지한다. 소프트웨어 및 구성 변경 내용은 표준 티켓팅 시스템을 사용하여 관리되고 추적된다.
보안 운영	**네트워크 설계**. Citrix 는 고객 콘텐츠 액세스에 대한 네트워크 제어를 비롯하여 액세스 관리 정책 및 표준을 서비스 전체에 적용하도록 설계된 메커니즘을 구현한다. 여기에는 인터넷과 내부 네트워크 사이에 신뢰할 수 없는 중간 영역을 구성하여 액세스 및 무단 트래픽을 제한하는 보안 메커니즘과 웹 및 응용 프로그램 서버와 해당하는 데이터베이스 서버를 계층화된 구조로 분리하여 두 계층 간의 트래픽을 제한하는 메커니즘이 포함된다.
인시던트 관리	**인시던트 대응**. Citrix는 Citrix 관리 네트워크 및/또는 시스템이나 고객 콘텐츠에 영향을 미치는 보안 및 안전 관련 인시던트를 억제, 분석, 해결 및 전달하도록 설계된 인시던트 대응 프로그램을 유지한다. **인시던트 알림**. 제어 범위에 포함되는 고객 콘텐츠가 보안 인시던트의 대상이 되었다고 판단되는 경우 Citrix는 준거법에 의해 요구되는 기간 내에 고객에게 알림을 제공한다. **인시던트 기록**. Citrix는 알려진 보안 인시던트의 기록을 인시던트 설명, 기간, 인시던트 결과, 보고자 이름, 인시던트를 보고받은 사람, 데이터 및 서비스 복구 절차와 함께 유지한다.
공급업체 관리	**온보딩**. Citrix 는 고객 콘텐츠 및/또는 고객 콘텐츠를 처리하는 서비스 구성 요소에 액세스하는 서비스 공급자의 보안 평가를 수행한다. Citrix 서비스에 연결하는 서비스 공급자는 이 절에서 해당 서비스 공급자가 제공하는 서비스에 해당하는 보안 수준을 준수해야 한다. 유럽 연합법이 적용되는 고객 콘텐츠에 액세스하는 서비스 공급자는 EU-미국 및 EU-스위스 개인 정보 보호 협약 프로그램을 자체 인증하거나 표준 계약 조항을 이행해야 한다. **지속적인 유지 관리.** 서비스 공급자는 제공하는 서비스의 중요도 및 위험에 따라 주기적으로 평가된다. **오프보딩.** 공급업체 관계가 종료된 서비스 공급자는 보유한 모든 고객 콘텐츠를

영역	제어
	반환하거나 모든 고객 콘텐츠가 안전하게 폐기되었음을 입증해야 한다.
비즈니스 지속성 및 재해 복구	**비즈니스 지속성.** Citrix 는 고객 콘텐츠를 처리하는 Citrix 정보 시스템이 위치한 시설에 대한 긴급 및 대체 계획을 유지한다. **재해 복구.** Citrix 의 중복 스토리지와 이러한 스토리지의 데이터 복구 절차는 고객 콘텐츠를 원래 상태 또는 마지막으로 복제된 상태로 재구성하도록 설계되었다.
고객의 보안 의무	고객은 서비스에 명시적으로 포함되지 않은 보안을 관리할 책임이 있다. 여기에는 다음이 포함되며 이에 국한되지 않는다. • 고객 콘텐츠에 대한 Citrix의 액세스를 고객이 서비스를 받는 데 필요한 범위로 제한한다. • 네트워크 및 컴퓨팅 장비를 모니터링하고 보호하는 등 네트워크 및 서비스 구성 요소에 간섭이 발생하지 않도록 한다. • 필요한 경우 서비스 기간과 서비스 종료 시에 고객 콘텐츠를 다운로드한다. • Citrix는 전송 중인 데이터를 기본적으로 암호화하거나 전송 중인 데이터를 암호화할 수 있는 수단을 고객에게 제공한다. 자세한 내용은 서비스에 대한 제품 설명서에 제공되어 있다. 고객은 전송 중인 데이터가 적절히 보호되는지 확인할 책임이 있다.

1.B. 추가 클라우드 서비스 보안 제어

영역	제어
데이터 보호 (가용성 제어, 전송 제어, 데이터 삭제)	**장애 조치(failover) 절차.** Citrix 는 고객 콘텐츠의 고객 콘텐츠의 복사본을 고객 콘텐츠를 처리하는 기본 컴퓨터 장비가 있는 장소와 다른 장소에 저장하는 메커니즘을 포함하여 가용성 손실을 해결하는 메커니즘을 구현한다. **경계를 벗어나는 데이터.** Citrix 는 서비스의 일부로 공용 네트워크를 통해 전송되는 고객 콘텐츠를 암호화하거나 고객이 암호화할 수 있도록 한다. **보존.** Citrix는 법적인 이유로 필요한 경우 서비스 기간 이후에 고객이 액세스할 수 있도록 보관하여 고객 콘텐츠를 보존할 수 있다. Citrix는 본 별첨의 요구 사항을 이러한 고객 콘텐츠가 영구적으로 삭제되기 전까지 준수한다. 아래의 반환 절이 직접 적용되는 경우 Citrix는 서비스 종료 이후 고객 콘텐츠를 보존할 의무가 없다. **반환.** 이용 가능 여부와 해당하는 서비스 설명서에 따라 고객은 만료 후 30일 안에 고객 콘텐츠를 다운로드해야 한다.

영역	제어
	데이터 삭제. Citrix는 법적으로 더 이상 필요하지 않은 고객 콘텐츠를 안전하게 삭제한다.
보안 운영	**이벤트 로깅.** Citrix 는 특정 서비스에서 로그를 수집한다. 로그에는 액세스 ID, 시간, 부여되거나 거부된 권한, 진단 데이터(예: 추적 및 충돌 파일) 및 기타 관련 작업이 포함될 수 있다. 로그는 **(i)** 서비스 및 관련 분석을 제공하고, 보호하고, 관리하고, 측정하고, 개선하기 위해 사용되고 **(ii)** 고객 및 고객의 사용자의 지시에 따라 사용되며 **(iii)** Citrix 정책, 준거법, 규정 또는 정부의 요청을 준수하기 위해 사용된다. 여기에는 서비스 및 관련 구성 요소의 성능, 안정성, 사용 현황 및 보안에 대한 모니터링이 포함될 수 있다. 고객은 이러한 모니터링을 차단하거나 방해할 수 없다. Citrix 는 위에 명시된 목적을 위해 타사에서 수집한 정보로 로그를 보완할 수 있다. 로그는 본 별첨에 명시되지 않은 목적으로 사용될 수 있으며 집계된 형태로만 사용된다.
비즈니스 지속성 및 재해 복구	**백업.** 해당하는 서비스 설명서에 달리 명시되지 않은 한 서비스는 다수의 물리적 사이트에 걸쳐 있는 고가용성의 활성-활성 클러스터에 유지된다. 활성-활성 구성에 유지되지 않는 시스템은 특정 서비스의 서비스 수준 목표에 따라 백업된다.

2조. 개인 데이터의 처리

개인 데이터는 식별되거나 식별 가능한 개인에 대한 정보이다. 고객 콘텐츠에 포함되는 개인 데이터는 고객이 결정한다. 서비스를 수행함에 있어서 Citrix는 고객 콘텐츠에 포함된 모든 개인 데이터에 대한 데이터 처리자 역할을 하며 고객은 이러한 데이터에 대한 데이터 제어자로 유지된다. Citrix는 본 계약에 명시된 것과 같이 이러한 개인 데이터의 처리에 관한 고객의 지침에 따라 행동한다.

이러한 데이터의 해외 전송에 사용되는 메커니즘을 포함하여 일반 데이터 보호 규정이 적용되는 개인 데이터의 처리에 관한 추가 정보는 별첨 I 일반 데이터 보호 규정 약관에 나와 있다.

3조. 서비스 위치

고객 콘텐츠는 미국 또는 Citrix 및/또는 해당 서비스 공급자가 운영하는 기타 국가로 전송되어 저장 및/또는 처리될 수 있다. 본 별첨의 요구 사항은 Citrix가 고객 콘텐츠를 저장하거나 처리하는 위치와 관계없이 적용된다.

양 당사자는 Citrix의 서비스 제공과 관련된 합법적인 데이터 해외 전송을 용이하게 할 선의의 목적으로 추가 데이터 처리 또는 데이터 전송 계약을 협상할 수 있다.

4조. 고객 콘텐츠의 공개

고객은 이 절에 명시된 대로 Citrix가 고객 콘텐츠를 공개하는 데 동의한다.
Citrix는 하청계약자 및 대리인을 통해 서비스를 수행할 수 있다. 모든 하청계약자 및 대리인은 서비스를 수행하는 데 필요한 경우에만 고객 콘텐츠에 액세스할 수 있으며 Citrix가 본 별첨에서 요구하는 데이터 보호 수준 이상을 제공하도록 명시한 서면 계약의 적용을 받는다. Citrix는 하청계약자와 대리인이 항상 본 계약의 약관을 준수하는지 확인할 책임이 있다.

또한 Citrix는 고객 콘텐츠를 (a) 본 계약과 일치하는 목적으로 계열사에 공개하거나 (b) 비즈니스의 일부 또는 전체에 대한 예상 또는 실제 합병, 인수, 매각, 파산 또는 기타 구조 조정과 관련하여 본 계약의 약관에 따라 고객 콘텐츠를 보호할 의무를 다하기 위해 공개하거나, (c) 권리 행사, 부정 행위 감지 및 예방, Citrix, 고객, 사용자 또는 대중의 권리 또는 재산을 보호하는 등의 법적인 용도로 공개하거나, (c) 소환, 재판 또는 행정 명령이나 구속력을 가진 기타 기구의 요청에 응해야 하는 경우 등 법률에 의해 요구되는 경우(각각 "요구") 공개할 수 있다. 법적으로 금지되는 경우를 제외하고 Citrix는 즉시 고객에게 이러한 요구를 알리고 고객이 적시에 요구에 응하는 데 필요한 고객 지원을 적절히 제공한다.

5조. 고객의 의무

1. 일반. 고객은 본 계약이 허용하는 대로만 서비스를 사용하고 액세스할 수 있다. 고객은 서비스 사용과 관련하여 해당하는 모든 법률을 준수한다.

2. 권한. 고객은 Citrix가 본 별첨에 명시된 대로 고객 콘텐츠에 액세스하고 처리하는 데 필요한 모든 고지를 제공하고 필요한 모든 동의 또는 라이센스를 구하는 등 Citrix가 서비스를 수행하는 데 필요한 모든 권한을 얻을 책임이 있다.

3. 규제. 고객은 본 별첨을 포함하여 계약에 명시된 것 이외에 추가로 적용되는 규제 또는 보안 요구 사항이 고객 콘텐츠에 적용되는지 여부를 확인할 책임이 있다. 고객은 미국 국제무기거래규정(ITAR) 또는 방산물자나 방산 서비스의 수입이나 수출을 제한하는 국가의 유사 규정이 적용되는 고객 콘텐츠를 제출하거나 저장하지 않는다. 또한 고객은 고객의 주문 및 해당하는 서비스 설명서에 명시되지 않은 한 개인의 건강 정보(Protected Health Information "PHI"), 결제 카드 정보(Payment Card Information, "PCI"), 정부 규제에 따른 데이터 배포 통제 등의 추가 규제 요구 사항이 적용되는 고객 콘텐츠를 제공하거나 저장하지 않으며 양 당사자는 Citrix가 이러한 데이터를 처리하는 데 필요할 수 있는 추가 계약[예: BAA(비즈니스 제휴 계약)]을 사전에 체결하였다. ShareFile 서비스의 고객은 privacy@sharefile.com으로 Citrix에 문의하여 BAA를 요청할 수 있다.

4. 고객 보안 환경. 서비스는 대규모 고객 보안 환경 내에서만 제공되도록 설계되었다. 고객은 서비스와 함께 사용되는 액세스 제어, 방화벽, 응용 프로그램 및 네트워크 등 Citrix가 명시적으로 관리하지 않는 모든 구성 요소의 보안 기능이 적절한지 확인해야 한다. 상기의 1.A.절 고객의 보안 의무를 참조한다.

5. 보안 알림. 고객은 서비스 및/또는 고객 콘텐츠가 관련된 보안 인시던트가 발생할 경우 아래의 VI조 Citrix 연락처에 명시된 대로 즉시 Citrix에 알려야 한다.

6. 사용자 규정 준수. 고객은 사용자가 주문 및 본 계약의 약관을 준수하도록 할 책임이 있다.

6조. **Citrix 연락처**

직무	연락처
고객 지원	https://www.citrix.com/contact/technical-support.html
인시던트 보고	secure@citrix.com
Citrix 제품의 의심되는 취약점	secure@citrix.com

7조. **정의**

본 별첨에 포함된 주요 용어의 의미는 계약 또는 아래에 명시되어 있다. 계약의 나머지 약관과 아래의 정의가 상충하는 경우 본 별첨에는 아래의 정의가 적용된다.

고객 콘텐츠는 저장을 위해 고객 계정에 업로드된 데이터 또는 Citrix가 서비스 수행을 위해 액세스 권한을 제공받은 고객 컴퓨팅 환경의 데이터를 말한다.

로그는 서비스와 관련된 이벤트의 기록을 의미하며 성능, 안정성, 사용 현황, 보안 및 지원을 측정하는 기록이 포함된다.

보안 인시던트는 고객 콘텐츠의 기밀성, 무결성 또는 가용성을 손상하는 무단 액세스를 말한다.