

Dell APEX 정보 보안 조치 부록

Dell APEX 서비스는 해당 서비스가 귀하의 구내 또는 코로케이션 현장에서 호스팅되지만, Dell 이 관리하는 데이터 센터의 서버에서 일반적으로 고객 콘텐츠를 호스팅하지 않는 것을 내용으로 하므로, 귀하와 Dell 각자가 특정한 책임을 지는 공동 보안 책임 모델을 사용합니다. 귀하의 책임은 관련 서비스 제공 상세에 명시되어 있습니다.

Dell 은 Dell APEX 서비스를 위한 다음의 회사 보안 조치를 구현하고 유지 관리합니다. 이러한 조치는 관련 서비스 제공 상세에 명시된 보안 조치와 함께 Dell APEX 서비스 보안과 관련된 Dell 의 유일한 책임에 해당합니다. 본 문서에 달리 정의하지 않는 한 본 문서에 사용된 모든 대문자로 표기된 용어는 APEX 계약에서 부여된 의미를 가집니다.

기능	조치
정보 보안 프로그램	<p>Dell 은 다음을 목적으로 설계된 정보 보안 프로그램(내부 정책 및 표준의 채택 포함)을 구현했으며 향후에도 유지할 계획입니다.</p> <p>(a) Dell APEX 서비스("Dell 네트워크")를 제공하는 데 사용되는 Dell 기업 데이터 센터, 서버, 네트워킹 장비, 방화벽 및 호스트 소프트웨어 시스템의 일부(해당되는 경우)에 대한 합리적으로 예측 가능한 보안 위험을 식별할 목적</p> <p>(b) 정기적인 위험 진단 및 테스트를 포함하여 Dell 이 적절하다고 판단하는 방식으로 Dell 네트워크에 대한 식별된 보안 위험을 완화하기 위해 상업적으로 합당한 노력을 기울일 목적</p> <p>Dell 은 정보 보안 프로그램의 조정, 모니터링 및 시행을 담당하는 한 명 이상의 보안 책임자를 임명했습니다.</p> <p>Dell 은 Dell 네트워크의 취약성을 지속적으로 모니터링하는 위험 및 취약성 관리 프로그램을 유지할 것입니다. 취약성은 다양한 자료/방법(공급업체, 보안 연구원, 취약성 점검, 레드팀 활동, 침투 테스트 및 직원 신고 등이 포함될 수 있음)을 사용하여 식별합니다. 공개된 제 3 자 취약성은 Dell 환경에 적용 가능한지 검토를 거칩니다. 취약성 점검 및 평가는 Dell 의 애플리케이션 인프라스트럭처에서 일상적이고 정기적으로 수행됩니다. 해당 절차들은 Dell 의 규정 준수 및 규제 요건을 지원할 뿐만 아니라 취약성을 사전에 식별하고 해결할 수 있도록 설계되었습니다.</p>
보안 개발 수명 주기 및 취약성 대응	<p>Dell 은 보안 개발 수명 주기가 정의된 공식 거버넌스 프로그램의 구조에 따라 오퍼링이 적절하게 평가, 개발 및 패키징되도록 취해야 할 단계를 정의하기 위해 보안 개발 수명 주기 프로그램을 구현하고 유지 및 관리합니다. 해당 프로그램은 Dell 의 정보 보안 프로그램과 더불어 Dell APEX 시스템의 개발 및 유지 관리 수명 주기 전반에 걸쳐 보안 문제를 해결하는 데 도움이 됩니다. Dell 은 보안</p>

	<p>개발 및 취약성 대응 사례를 지속적으로 평가하고 개선하기 위해 엄격한 프로세스를 사용하며, 이를 업계 표준 사례와 정기적으로 비교 대조합니다.</p> <p>Dell은 Dell APEX 시스템에서 판명된 취약성을 조사하고 검증한 후 Dell에서 게시한 취약성 대응 정책(현재 https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy에서 확인 가능)에 따라 적절한 보상책을 식별, 개발 및 검증하고자 노력합니다.</p> <p>해당되는 경우 Dell은 보안 권고의 방식으로 고객에게 보상책을 전달합니다. 해당되는 경우 Dell은 상업적으로 합당한 시간 내에 보상책을 제공하기 위해 노력을 기울입니다. 대응 일정은 심각도, 보상책의 복잡성 또는 영향을 받는 구성 요소와 같은 여러 요인에 따라 달라질 수 있습니다.</p>
<p>자산 관리</p>	<p>Dell은 Dell 네트워크의 물리적 및 논리적 자산을 추적하고 관리합니다. Dell이 추적할 수 있는 자산 및 실행할 수 있는 통제의 예는 다음과 같습니다.</p> <ul style="list-style-type: none"> (a) 소프트웨어 자산(예: 애플리케이션 및 시스템 소프트웨어) (b) 물리적 자산(예: 서버, 데스크탑/노트북, 백업/보관 테이프, 프린터 및 통신 장비) (c) 정보 자산(예: 데이터베이스, 재해 복구 계획, 비즈니스 연속성 계획, 데이터 분류, 보관 정보) <p>Dell은 비즈니스 중요도 및/또는 데이터 분류 민감도를 기준으로 자산을 분류합니다. 이러한 분류를 통해 해당 자산에 대한 액세스를 적절하게 제한할 수 있습니다.</p>
<p>인적 자원 보안</p>	<p>고용 프로세스의 일환으로 Dell 직원은 채용 시 NDA(Non-Disclosure Agreement)에 서명하고 관련 법률에 따라 심사 절차를 거쳐야 합니다. Dell은 단독 재량에 따라 자체 정책을 검토하고 직원 보안을 구현할 권한이 있지만, 현재 정책과 현지 법률 및 현지 사정에 따라 Dell은 약물 사용 기록 조사, 사회 보장 기록 추적, 범죄 회보, 교육 및 취업 내역 확인, 취업 자격 확인 등과 같은 고용 심사 중 하나 이상을 수행합니다. Dell은 Dell이 속한 업계의 여타 기업에서 현재 적용하는 업계 표준을 충족하려고 노력하지만, 특정 고객의 특정 기대치를 충족하는 직원 보안 또는 심사 프로세스를 구축할 수는 없습니다.</p> <p>타사나 외부 계약자는 Dell의 심사를 받거나, 계약 조건에 따라 심사를 받거나, Dell에서 승인한 심사 프로세스에 따른 계약자의 심사를 통해 검증받을 수 있습니다.</p> <p>Dell은 정보 보안 프로그램 요구 사항을 준수하지 않는 직원에 대해 조치를 취하는 징계 절차를 유지합니다. 여기에는 보안, 가용성, 기밀 유지 약정 및 요건을 충족하기 위해 마련된 프로세스가 포함되나 이에 국한되지 않습니다.</p>

	<p>Dell은 모든 관련 직원에게 연간 보안 인식 교육을 제공하며, 관련 하청업체에도 그 직원에게 동일한 교육을 제공할 것을 요구합니다.</p>
<p>물리적 보안</p>	<p>Dell은 Dell 네트워크의 물리적 구성 요소가 있는 시설에 대한 물리적 액세스를 인가된 직원으로 한정하고 해당 시설로의 무단 진입을 방지하는 정책 및 통제 조치를 유지 및 관리합니다.</p> <p>Dell 네트워크의 물리적 구성 요소를 수용하는 시설(예: 데이터 센터)에는 위험 기반 통제 조치가 마련되어 있습니다. 액세스 제어 조치에는 보안 경비, 보안 기록, 모니터링, 경보, 보안 영역에의 액세스 제한, 액세스 경로 보호, 영상 관제, 키 카드 및/또는 2 단계 인증이 포함될 수 있습니다.</p> <p>이 조항은 Dell 이 관리하는 코로케이션 현장에 적용됩니다.</p>
<p>네트워크 보안</p>	<p>Dell 은 Dell APEX 서비스를 제공하는 데 필요한 경우 Dell 네트워크에 전자적으로 액세스할 수 있습니다. Dell 은 각 연결을 통해 Dell 네트워크로 허용되는 액세스를 관리하기 위해 방화벽 사용 및 인증 통제를 비롯한 정책 및 액세스 제어 조치를 유지 관리합니다.</p> <p>Dell 은 위험을 고려하여 통제 조치를 실시함으로써 Dell 네트워크 내 악의적인 자산 사용과 악성 소프트웨어를 방지합니다. 이러한 통제 조치는 보안 정책, 제한적 액세스 제어, 별도의 개발 및 테스트 환경, 서버, 데스크탑 및 노트북의 멀웨어 탐지, 멀웨어 이메일 첨부 파일 검사, 시스템 규정 준수 점검, 침입 방지 모니터링 및 대응, 의심스러운 주요 이벤트에 대한 로깅 및 알림, 데이터 유형별 정보 처리 절차, 전자상거래 애플리케이션 및 네트워크 보안, 외부 자산 사용, 시스템 및 애플리케이션 취약성 검사를 포함하되 이에 국한되지 않습니다.</p> <p>필요한 경우 및 정보 보안 프로그램에 따라 Dell 은 전송 중인 데이터 및 저장된 데이터의 암호화를 요구합니다. Dell 은 공개 네트워크를 통해 고객 시스템에 원격으로 액세스하는 경우 암호화 및 적절한 프로토콜(예: TLS)을 사용합니다. Dell 은 암호화 키가 사용되지 않을 경우 업계에서 인정하는 키 관리 방식을 제공하도록 설계된 공인 솔루션에 해당 키를 저장합니다.</p>
<p>액세스 제어</p>	<p>Dell 은 Dell 네트워크에 대한 무단 액세스를 방지하기 위한 적절한 액세스 제어 조치를 구현합니다. 고의 여부와 관계없이 오용이나 기타 오용의 위험을 줄이기 위해 "최소 권한" 및 "인가 범위(need to know)"의 원칙에 따라 액세스를 제어합니다. Dell 에서 활용할 수 있는 액세스 제어에는 액세스 권한 검토, 애플리케이션에 대한 권한 있는 액세스 및 서비스 계정 유지 관리, 액세스를 위한 시스템 수준 설정 및 액세스 관련 보고서 생성이 포함됩니다.</p> <p>해당되는 경우 Dell 은 2 단계 인증을 비롯한 업계 표준 방식을 활용하여 Dell 네트워크 사용자를 식별하고 인증합니다. Dell 은 Dell 네트워크 전반에서 강력한 비밀번호 사용을 요구합니다. Dell 은 (a) Dell 네트워크 사용자가 비밀번호를 공유하거나, 기록하거나, 이메일로 보내거나, IM 으로 보내거나,</p>

	<p>시스템에 암호화하지 않고 저장하는 것을 금지하며, (b) 잘못된 비밀번호를 연속하여 사용 시도할 경우 계정을 잠급니다.</p> <p>Dell 은 업계 표준 관행을 활용하여 액세스 제어 조치를 강화합니다. 해당 조치에는 다음이 포함됩니다.</p> <ul style="list-style-type: none"> (a) 유효 상태인 사용자 세션에 대해 자동 시간 초과 처리 (b) 재개설의 경우 본인 확인 및 비밀번호 요구 (c) 인터넷 연결(해당되는 경우)이 VPN 연결로 보호되는 공인 업계 표준 방화벽을 통해 외부 액세스로부터 보호 (d) 적절하게 표시되거나 입력된 비밀번호를 마스킹 처리 (e) 전송 시 비밀번호를 적절한 업계 표준에 따라 암호화
<p>사고 관리</p>	<p>Dell 은 사고 대응 체계를 활용하여 보안 이벤트에 대비, 대처하고 이를 관리하며 해당 이벤트의 영향을 최소화합니다. 해당 체계에는 다음과 같은 절차가 포함되며, 보안 사고 발생 시에는 이를 따라야 합니다.</p> <ul style="list-style-type: none"> (a) 대응 담당자가 배치된 내부 사고 대응 팀 (b) 근본 원인 분석을 수행하고 영향을 받는 당사자를 식별하는 조사 팀 (c) 내부 보고 및 통지 프로세스 (d) 대응 조치 및 문제 해결 계획 문서화 (e) 사고 사후 검토
<p>비즈니스 연속성 관리</p>	<p>Dell 은 합리적인 선에서 가급적 조속히 비즈니스 중단을 복구하고 정상적인 비즈니스 운영을 재개하기 위한 비즈니스 연속성 계획("BCP")을 유지 관리합니다. Dell 은 Dell APEX 서비스에 상당한 영향을 주는 비즈니스 중단 발생 시 상황에 따라 적절하고 신속한 방식으로 귀하에게 연락하려고 시도합니다.</p>