CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

U.S. Customs and Border Protection
미국국토안보부

최소 보안 기준 – 외국 제조업체

2020 년 1 월

유의 사항: 기준 ID 번호가 순차적이지 않을 수 있습니다. 목록에 들어 있지 않은 ID 번호는 외국 제조업체에 적용되지 않습니다.

첫 번째 집중 영역: 기업 보안

1. 보안 비전 및 책임 – CTPAT 회원의 공급망 보안 프로그램이 효과적이고 그렇게 유지되기 위해서는 회사 고위 경영진의 지원이 필요합니다. 회사 문화의 필수적인 부분으로써 보안 프로그램을 설치하고 그것을 회사 전체의 우선 사항으로 하는 것은 대체로 회사 지도부의 책임입니다.

ID	기준	시행 안내	필수/ 권장
1.1	보안 문화를 촉진하는 데 있어 CTPAT 회원은 공급망 보안과 CTPAT 프로그램에 대한 헌신을 지원 진술서를 통해 보여주어야 합니다. 그 진술서는 회사 고위 책임자에 의해 서명이 되고 적절한 회사 위치에 전시되어야 합니다.	지원 진술서는 공급망을 마약 밀매, 테러리즘, 인신 매매 그리고 불법 밀수품과 같은 범죄 활동으로부터 보호하는 것이 중요하다는 것을 강조해야 합니다. 진술서에 지원을 표현하고 서명하는 고위 회사 책임자의 예로 사장, CEO, 부장 혹은 보안 국장을 들 수 있습니다. 지원 진술서가 전시될 수 있는 장소의	권장

ID	기준	시행 안내	필수/권장
		예로 회사 웹사이트, 회사 주요 공간(리셉션, 포장, 창고 등) 내 포스터 그리고/또는 회사 보안 세미나 등을 들 수 있습니다.	
1.2	강력한 공급망 보안 프로그램을 만들기 위해 회사는 모든 관련 부서의 대표를 모아 교차 기능팀을 만들어야 합니다. 이 새로운 보안 조치는 기존 회사 절차의 일부가 되어야 하는데, 그렇게 했을 때보다 지속가능한 구조가 형성되고 공급망 보안이 모든 사람의 책임이라는 사실이 강조됩니다.	공급망 보안은 종전 보안 프로그램보다 더 폭넓은 범위에서 이루어집니다. 이것은 인사, 정보 기술 그리고 수입/수출 부서와 같은 여러 부서에서의 보안과 밀접하게 관련됩니다. 보다 종전 보안 부서 모델에 기초한 공급망 보안 프로그램의 경우 장기적으로는 실행 가능성이 떨어지는데, 그 이유는 보안 조치를 실행할 책임이 적은 수의 직원에게 집중되어 있어, 주요 직원이 없는 경우에 취약해질 수 있습니다.	권장
1.3	공급망 보안 프로그램은 문서로 된 적절한 검토 요소에 의해 지원을 받을 수 있도록 설계되고 지원받으며 실행될 수 있어야 합니다. 이 검토 요소의 목적은 직원이 자신의 맡은 직무를 제대로 수행하고 있는지 확인하고 보안 프로그램에 요약 기술된 모든 보안 절차가 계획대로 실행이 되는 체계가 있다는 것을 문서로 기록하는 것입니다. 검토 계획은 조직의 운영과 위험 수준에 따라 필요 시 갱신되어야 합니다.	CTPAT 검토의 목적은 직원이 회사의 보안 절차를 반드시 따르도록 하는 데 있습니다. 검토 과정이 복잡할 필요는 없습니다. 회원이 자사의 공급망, 사업 모델, 위험 수준 그리고 구체적인 장소/현장 간의 차이를 고려해 검토 범위와 함께 얼마나 심도있게 검토를 할 것인지를 결정하게 됩니다. 규모가 작은 회사는 아주 간단한 검토 방식을 만드는 반면 규모가 큰 다국적 대기업의 경우보다 긴 과정이 필요하고 지역의 법적 요건 등과 같은 다양한 요인을 고려해야 할 수 있습니다. 일부 큰 회사는 이미 보안 검토에 도움을 줄 수 있는 감사 직원을 두고 있습니다. 회원은 특정한 절차를 겨냥한 소규모 선별 검토를 선택할 수 있습니다. 검사와 봉인 통제와 같은 공급망 보안에 중요한	필수

ID	기준	시행 안내	필수/ 권장
		특화된 영역의 경우 그 영역에 대한 특정한 검토를 할 수 있습니다. 그러나 보안 프로그램 전 영역이 설계된 대로 운영될 수 있도록 전체 일반 검토를 주기적으로 하는 것이 좋습니다. 회원이 이미 검토를 연례 검토의 일부로 하는 경우 그 과정이 이 기준을 만족시킬 수 있습니다. 위험이 높은 공급망(위험 평가의 결과)을 지닌 회원은 실제 보안 사고 시 모든 직원이 어떻게 대응할지 알 수 있도록 시뮬레이션이나 테이블톱 훈련을 검토 프로그램에 포함할 수 있습니다.	
1.4	회사의 CTPAT 연락 담당자(POC)는 CTPAT 프로그램 요건에 대해 잘 알고 있어야 합니다. 이들은 모든 감사, 보안 관련 연습 그리고 CTPAT 인증과 같은 프로그램에 대해 고위 경영진에 정기적으로 업데이트를 해주어야 합니다.	CTPAT 가 기대하는 지정된 연락 담당자는 활동적이며 자신의 공급망 보안 전문가와 연락을 취하고 그들에게 신속하게 반응하는 능동적인 사람입니다. 회원은 이 기능을 지원할 수 있는 추가 직원을 CTPAT 포털에 연락 담당으로 올려 알려줄 수 있습니다.	필수

2. <u>위험 평가</u> – 공급망을 겨냥한 테러 집단과 범죄 조직의 계속된 위협은 회원이 이런 진화하는 위협에 대한 현재 노출 상태 혹은 노출 가능성을 평가하는 것이 중요하다는 것을 알게 해 줍니다. 회사가 많은 사업 파트너를 가진 복수의 공급망을 지닌 경우, 그런 공급망을 확보하는 것이 더욱 복잡해진다는 것을 CTPAT 는 알고 있습니다. 회사가 많은 공급망을 지닌 경우 더 높은 위험을 지닌 지리적 영역/공급망에 집중해야 합니다.

자신의 공급망 내 위험 수준을 판단할 때 회원은 사업 모델, 공급자의 지역적 위치 그리고 특정 공급망에만 존재할 수 있는 기타 다른 측면과 같은 다양한 요인을 고려해야 합니다.

주요 정의: 위험 – 위협, 취약점 그리고 결과를 포함한 바람직하지 못한 사건으로부터 발생할 수 있는 피해 정도. 위험 수준을 결정하는 것은 위협 발생 가능성이 얼마나 높은가 하는 것입니다. 보통 높은 발생 가능성은 높은 위험 수준을 말합니다. 위험을 제거할 수는 없지만, 취약점이나 사업에 끼치는 전반적인 영향을 줄이는 식의 관리로 그 위험을 줄일 수 있습니다.

ID	기준	시행 안내	필수/ 권장
2.1	CTPAT 회원은 공급망 내 위험 수준을 측정하고 문서로 기록해야 합니다. CTPAT 회원은 어디가 보안 취약점인지 알아보기 위해 전반적인 위험 평가(RA)를 해야 합니다. RA 는 위협을 찾아내고 위험을 평가하며 취약점을 줄이기 위해 유지 가능한 조치를 포함해야 합니다. 회원은	전반적인 위험 평가(RA)는 두 주요 부분으로 되어 있습니다. 첫 번째 부분은 회원이 통제하는 시설 내 회원의 공급망 보안 실행, 절차 그리고 정책에 대한 자가 평가로 이것은 회원이 CTPAT 최소 보안 기준을 준수하는지 그리고 위험을 어떻게 관리하고 있는지에 대한 경영진의 전반적인 검토를 확인하기 위한 것입니다. RA 의 두 번째 부분은 국제 위험 평가입니다. RA 의 이 부분에는 공급망 내 회원의 사업 모델과 역할에 기초한 지리적 위협을 찾아내는 것이 포함됩니다. 회원의 공급망 보안에 대한 모든 위협으로 인한 영향을 고려할 때 회원은 다른 수준의 위험을 평가하고 구별해주는 방법을 사용해야 합니다. 간단한 방법으로 위험 정도를 "낮음" "중간" 그리고	필수

ID	기준	시행 안내	필수/권장
	공급망에서 회원의 역할에 대한 구체적인 CTPAT 요건을 고려해야 합니다.	"높음"으로 구분할 수 있습니다. CTPAT 는 회원의 전반적인 위험 평가 중 국제 위험 평가 부분을 실시하는 데 도움을 주기 위해 "5 단계 위험 평가" 가이드를 만들었는데, 그것은 다음 미국 관세국경보호청 웹사이트에 나와 있습니다: https://www.cbp.gov/sites/default/files/documents/C-TPAT%27s%20Five%20Step%20Risk%20Assessment%20Process.pdf. 넓은 공급망을 지닌 회원의 경우 위험이 높은 영역에 먼저 집중할 것을 권합니다.	
2.2	위험 평가의 국제 부분에는 원산지부터 수입자의 배송 센터까지 공급망 전체에 걸친 회원의 화물 이동이 기록되거나 도표화되어야 합니다. 도표에는 물품의 수출/이동에 직·간접적으로 관련된 모든 사업 파트너가 포함되어야 합니다. 필요한 경우 도표에는 화물이 어떻게 운송 시설/화물 거점에 들어가고 나오는지에 대한 기록과 함께 화물이 이 장소 중 한 군데서 장기간 "휴지"하고 있는 경우, 거기에 대한 메모가 포함되어야	공급망을 도표화하는 과정을 개발할 때는 높은 위험 영역을 먼저 고려해야 합니다. 화물의 움직임을 기록할 때 회원은 관세사와 화물을 직접 다루지는 않지만, "무선박운송인 제도"(NVOCC)나 제 3 자 물류업체(3PL)와 같은 운영 통제를 할 수 있는 사람과 같이 수입/수출 문서를 다루는 일만 하는 사람들을 포함해 관련 당사자 모두를 고려해야 합니다. 운송의 어느 일부라도 하도급을 준 경우에도 이것을 고려할 수 있는데, 간접 관련자 층이 많을수록 연루된 위험이 커지기 때문입니다. 도표화 작업의 일부는 귀하의 공급망이 어떻게 운영되는지 심도있게 들여다보는 것입니다. 위험을 찾아내는 것 이외에도 그것은 비효율적인 공급망을 지닌 영역을 찾아내는 역할도 하는데, 그 결과 제품을 받는 데 필요한 비용이나 리드 타임을 줄이는 방법을 찾아낼 수 있습니다.	권장

ID	기준	시행 안내	필수/권장
	합니다. 화물은 여정의 다음 구간으로의 이동을 기다리며 "휴지"하고 있을 때 더 취약합니다.		
2.3	위험 평가는 매년 혹은 위험 요인에 따라 더 자주 검토되어야 합니다.	위험 평가 검토가 일 년에 한 차례보다 더 자주 필요할 수 있는 상황의 예로 특정 국가로부터의 위협 수준 증가, 보안 침입이나 사고 후 강화된 경계, 사업 파트너의 변화 그리고/또는 병합 및 인수 등과 같은 기업 구조/소유권의 변화를 들 수 있습니다.	필수
2.4	CTPAT 회원이 위기 관리, 사업 연속성, 보안 회복 계획 그리고 사업 재개를 다루는 문서로 된 절차를 갖추고 있을 것을 권장합니다.	위기의 예로 사이버 공격, 화재 혹은 무장한 사람에 의한 운송 회사 기사 납치로 발생한 중단된 무역 데이터 이동을 들 수 있습니다. 위험 정도와 회원이 어디에서 사업을 하고 어디에 하도급을 주느냐에 따라, 비상 계획에 추가 보안 통보나 지원, 파괴되거나 도난당한 것을 회복하고 정상적인 운영 상태로 회귀하는 방법이 포함될 수 있습니다.	권장

3. 사업 파트너 – CTPAT 회원은 국내와 국외에서 다양한 사업 파트너와 관계를 맺고 있습니다. 화물 그리고/또는 수입/수출 문서화 작업을 직접 처리하는 사업 파트너의 경우, 이들 사업 파트너가 국제 공급망 전체를 통해 물류를 확보할 수 있도록 적절한 보안 조치를 갖추는 것이 회원에게는 중요합니다. 사업 파트너가 특정 기능에 대해 하도급을 주는 경우 등식에 복잡한 단계가 추가되는데, 공급망 위험 분석을 할 때 이 사항을 고려해야 합니다.

주요 정의: 사업 파트너 – 사업 파트너는 CTPAT 회원의 공급망을 통해 미국에 수입되거나 미국에서 수출하는 물품의 보안 관리망에 영향을 줄 수 있는 행위를 할 수 있는 개인이나 회사 모두를 말합니다. 회사의 국제 공급망 내에서 필요한 점을 충족시켜주는 서비스를 제공하는 어느 당사자든 사업 파트너가 될 수 있습니다. 이 역할에는 CTPAT 수입업자 혹은 수출업자 회원을 위해 혹은 그들을 대신해 화물 구매, 문서 준비, 처리, 보관 그리고/또는 이동하는 데 (직·간접적으로) 관련된 모든 당사자가 포함됩니다. 간접적인 파트너의 두 가지 예로 대리인이나 물류 제공자가 마련한 하도급 운송 회사와 해외 통합 물류 창고를 들 수 있습니다.

ID	기준	시행 안내	필수/권장
3.1	CTPAT 회원은 신규 사업 파트너를 검사하고 기존 파트너를 모니터링하는 문서화된 위험 기반 과정을 갖추고 있어야 합니다. 이 과정에서 회원이 포함할 것을 권하는 요인은 돈 세탁과 테러리스트 자금 지원과 관련된 행위를 점검하는 것입니다. 이 과정에 대해 도움을 받으려면 CTPAT 의 "무역 기반 돈 세탁과 테러리즘 자금 지원 활동 경고 지표"를 참고하십시오.	회사가 합법적인지 결정하는 데 도움을 줄 수 있는 일부 심사 요소의 예로 다음과 같은 것이 있습니다. • 회사의 사업장 주소와 그 주소에서 얼마나 오래 있었는지 확인하기 • 회사와 그 소유주에 대해 인터넷에서 찾아보기 • 사업 거래처 알아보기 • 신용 보고서 요청하기 검사가 필요한 사업 파트너에 제조업자, 제품 공급업자, 관련	필수

ID	기준	시행 안내	필수/권장
		벤더/서비스 제공자 그리고 운송/물류업체와 같은 직접적인 사업 파트너가 포함됩니다. 회사의 공급망에 직접 관련되고/되거나 민감한 정보/장비를 다루는 벤더/서비스 제공자 역시 검사 목록에 들어가는데, 여기에는 중개인이나 계약된 IT 제공자가 포함됩니다. 검사를 얼마나 심층적으로 하는가 하는 것은 공급망 내 위험 수준에 따라 달라집니다.	
3.4	사업 파트너 검사 과정에서는 파트너가 미국과의 상호인정 협정(MRA)(혹은 승인된 MRA)이 포함된 수출입 보안관리 우수 공인 업체(AEO) 프로그램 사업 파트너인지 그 여부가 고려되어야 합니다. CTPAT 나 승인된 AEO 인증은 사업 파트너가 프로그램 요건을 만족시킨다는 증거로서 받아들여지며, 회원은 인증의 증거를 확보해야 하며 이들 사업 파트너가 인증을 유지할 수 있도록 계속 모니터링해야 합니다.	사업 파트너의 CTPAT 인증 여부를 CTPAT 포털의 "상태 확인 인터페이스" 시스템을 통해 알아볼 수 있습니다. 사업 파트너의 인증이 미국과의 MRA 아래 외국 AEO 프로그램에 의한 것이라면 그 외국 AEO 인증에 보안 요소가 포함돼 있을 것입니다. 회원은 그 관세 관리 AEO 이름이 목록에 들어가 있는 외국 관세 관리 웹사이트를 방문하거나 사업 파트너에 직접 인증을 요청할 수 있습니다. 현재 미국과 MRA 를 맺고 있는 나라의 예로 다음과 같은 국가가 있습니다: 뉴질랜드, 캐나다, 요르단, 일본, 한국, 유럽 연합(28 회원국), 대만, 이스라엘, 멕시코, 싱가포르, 도미니카 공화국, 페루.	필수
3.5	CTPAT 회원이 공급망 요소에 대해 하도급을 주거나 계약을 체결하는 경우, 회원은 (방문이나 질문지 등을 통해) 이 사업 파트너가 CTPAT 의 최소 보안	수입업자와 수출업자는 공급망 활동의 상당한 부분을 하도급에 맡기는 경향이 있습니다. 수입업자(그리고 일부 수출업자와)는 보통 이런 거래에 있어 사업 파트너에 대해 영향력이 있으며, 필요한	필수

ID	기준	시행 안내	필수/권장
	기준(MSC)을 만족시키거나 넘어서는 보안 조치를 갖추고 있는지 실사를 해야 합니다.	경우 공급망 전체에 걸쳐 보안 조치를 실행할 것을 요구할 수 있는 당사자입니다. CTPAT 나 인정된 MRA 회원이 아닌 사업 파트너의 경우, CTPAT 회원은 실사를 해서 이들 사업 파트너가 프로그램 내 해당 보안 기준을 만족시킬 수 있게 해야 합니다(그런 영향력을 발휘할 수 있는 경우). 보안 요건 준수를 확인하기 위해 수입업자는 사업 파트너에 대해 보안 평가를 실시합니다. 사업 파트너의 보안 프로그램에 관련되어 얼마나 많은 정보를 수집해야 하는지 결정하는 과정은 회원의 위험 평가에 그 근거를 두는데, 공급망이 많은 경우 높은 위험 영역을 우선시해야 합니다. 사업 파트너가 MSC 를 준수하는지 여부는 몇 가지 방법을 통해 알아낼 수 있습니다. 위험 정도에 기초해 회사는 시설에서 현장 감사를 하거나 현장 감사를 할 계약자/서비스 제공자를 고용하거나 보안 질문지를 사용할 수 있습니다. 보안 질문지를 사용하는 경우, 위험 정도에 따라 수집할 상세 내용이나 증거의 양이 정해집니다. 높은 위험 지역에 위치한 회사에게 더 많은 상세 내용이 요구될 수 있습니다. 회원이 보안 질문지를 사업 파트너에게 보낼 때는 다음 항목의 요구를 고려하십시오. •작성한 사람의 이름과 직책 •작성 날짜 •문서를 작성한 사람의 서명 •*질문지의 정확성을 확인해 줄 수 있는 고위 회사 책임자, 보안	

ID	기준	시행 안내	필수/권장
		감독 혹은 허가받은 회사 대표의 서명 •준수 여부 결정에 대해 충분한 상세 내용 제공 •지역 보안 규약이 허용하는 경우 위험에 기초해 사진 증거, 정책/절차 사본 그리고 "국제 교역 도구" 점검 목록 그리고/또는 보안 요원 일지 같은 것을 기재한 양식 사본을 포함 *전자로 서명을 할 수 있습니다. 서명을 받아내거나 확인하는 것이 어려운 경우, 답변자가 이메일로 질문지의 타당성과 함께 답변과 뒷받침하는 증거가 상사/관리자(이름과 직책 필요)에 의해 승인되었다는 것을 증명할 수 있습니다.	

ID	기준	시행 안내	필수/권장
3.6	사업 파트너의 보안 평가에서 취약점이 발견된 경우, 그것을 최대한 빨리 처리하고 시기적절하게 시정해야 합니다. 회원은 증거 문서를 통해 결함이 완화되었다는 것을 확인해야 합니다.	시정에 무엇이 필요한가에 따라 시정에 걸리는 시간이 달라진다는 것을 CTPAT 는 알고 있습니다. 물리적 장비를 설치하는 것은 절차적 변화보다 보통 시간이 많이 걸리지만, 발견 즉시 보안 공백 문제를 다루어야 합니다. 예를 들어 손상된 울타리를 교체하는 것이 문제라면, 새로운 울타리 구매 과정이 즉각 시작되어야 하며(결함 처리) 현실적으로 가장 빠른 시점에 새로운 울타리로 교체(시정 행위)되어야 합니다. 연루된 위험 수준과 발견된 취약점의 중요성에 따라 어떤 문제의 경우 즉각적인 처리가 필요할 수 있습니다. 예를 들어 컨테이너의 보안을 위협하는 결함인 경우 되도록 빨리 문제를 처리해야 합니다. 증거 문서에 포함되는 예로 추가 보안 요원 계약 사본, 새로 설치한 보안 카메라나 침입 경보 사진 혹은 검사 점검 목록 사본 등을 들 수 있습니다.	필수

ID	기준	시행 안내	필수/권장
3.7	사업 파트너가 CTPAT 의 보안 기준을 계속 준수할 수 있도록 회원이 사업 파트너의 보안 평가를 정기적으로 혹은 상황이나 위험으로 인해 필요한 경우 갱신해야 합니다.	사업 파트너의 보안 평가를 주기적으로 검토하는 것은 강력한 보안 프로그램을 갖추고 제대로 실행되게 하는 데 중요합니다. 회원이 사업 파트너의 보안 프로그램 평가 갱신을 한 번도 요구한 적이 없다면, 회원은 한때 실행 가능했던 프로그램이 더 이상 효과가 없다는 것을 모르게 돼 회원의 공급망이 위험에 놓이게 됩니다. 파트너의 보안 평가를 얼마나 자주 검토할 것인가 하는 결정은 회원 위험 평가 과정에 따라 달라집니다. 위험도가 높은 공급망의 경우 위험도가 낮은 공급망보다 더 자주 검토를 하게 될 것입니다. 회원이 사업 파트너의 보안을 직접 방문해 평가한다면, 다른 방식의 필요한 방문이 주는 이점을 고려할 수 있습니다. 예를 들어 품질 관리 검사를 하는 직원이 보안 확인도 할 수 있게끔 교차 교육을 하는 것입니다. 자가 평가 갱신이 더 자주 요구되는 상황의 예로 원산국 내 높아진 위협 수준, 원산지 변화, 새로운 중요 사업 파트너(화물을 실제로 다루고 시설에 보안 서비스를 제공하는 등의 업무를 하는 업체)를 들 수 있습니다.	권장

ID	기준	시행 안내	필수/권장
3.8	미국 내로 들어오는 수송품에 대해 회원이 교통 서비스를 다른 고속도로 운송 회사에 하도급을 주는 경우, 회원은 CTPAT 인증 고속도로 운송 회사나 문서로 된 계약에 기술된 대로 회원을 위해 직접 일하는 고속도로 운송 회사를 이용해야 합니다. 최소 보안 기준(MSC) 요건 전체가 계약 조건에 포함되어야 합니다.	운송 회사는 하도급 운송 회사와 운전기사 목록을 화물을 수거해 수송하는 시설에 제공해야 합니다. 하도급 목록에 변경 사항이 있으면 즉시 관련 당사자에게 알려야 합니다. 서비스 제공 업체가 요건을 준수하고 있는지 검토할 때 회원은 하도급을 준 회사가 실제로 화물을 운송하고 허락 없이 또 하도급을 주지 않았다는 사실을 확인해야 합니다. 회원은 하도급 운송 업체를 한 하도급 단계로 제한해야 합니다. 예외적으로 다음 단계 하도급을 허용하는 경우, CTPAT 회원과 운송 회사는 그 적재물에 대해 또 하도급을 주었다는 것을 통보받아야 합니다.	필수

ID	기준	시행 안내	필수/권장
3.9	CTPAT 회원은 미국에 수입된 물품이 전부 혹은 일부 금지된 형태의 노동(즉, 강제, 수감, 노예 혹은 노예 아동 노동) 방식을 통한 채굴되거나 생산 혹은 제조되지 않도록 회사가 어떻게 하는지를 다루는 문서화된 사회 준수 프로그램을 최소한 갖추고 있어야 합니다.	민간 부문이 운영과 공급망에서 노동자의 권리를 보호하려는 노력이 노동법과 그 기준에 대한 이해를 증진시킬수 있으며 나쁜 노동 관행을 줄일 수 있습니다. 이러한 노력은 또한 노동자와 고용주가 더 나은 관계를 가질 수 있는 환경을 조성하며 회사의 순수익을 향상시킬 수 있습니다. 1930 관세법 307 절(19 U.S.C. § 1307)은 상품의 전부 혹은 일부가 외국에서의 강제 아동 노동을 포함해 강제 혹은 노예 아동 노동으로 채굴되거나 생산 혹은 제조된 경우 그 수입을 금하고 있습니다. 국제노동기구 제 29 호 협약은 강제 노동을 처벌의 공포 아래 이루어지고 상기된 사람이 자발적으로 제공하지 않은 모든 노동 또는 용역으로 정의하고 있습니다. 사회 준수 프로그램은 회사가 사회 및 노동 문제를 다루는 윤리 강령 요소를 최대한 준수할 수 있도록 제정된 일련의 정책과 관행입니다. 사회 준수는 사업체가 환경뿐만 아니라 고용인과 사업을 운영하는 지역의 건강과 보안과 권리 그리고 회사의 공급망 내에 있는 사람들과 지역을 보호하는 의무를 어떻게 다루는지에 관한 것입니다.	권장

4. <u>사이버 보안</u> – 오늘날 디지털 세상에서 사이버 보안은 무엇보다도 지식 재산, 고객 정보, 재정 및 무역 데이터 그리고 직원 기록 같은 회사의 가장 귀중한 자산을 보호하는 데 중요합니다. 인터넷 연결이 확대되면서 회사의 정보 시스템 침입 위험도 생깁니다. 유형과 규모에 상관없이 모든 사업이 이 위협에 노출될 수 있습니다. 회사의 정보 기술(IT)과 데이터는 가장 중요한 부분이며 아래에 열거된 기준이 회원의 전반적인 사이버 보안 프로그램에 대한 초석이 됩니다.

주요 정의: 사이버 보안 – 사이버 보안은 컴퓨터, 네트워크, 프로그램 그리고 데이터를 의도하지 않거나 허가하지 않은 접속이나 변경 혹은 파괴로부터 보호하는 것을 주로 하는 활동이나 과정입니다. 그것은 사이버 관련 위험을 찾아내고, 분석하며 접속하고 알리며, 동반된 비용과 혜택을 고려해 그것을 받아들일 수 있는 수준으로 받아들이거나 회피하거나 이전하거나 완화하는 과정을 말합니다.

정보 기술(IT) – IT에는 컴퓨터, 저장 공간, 네트워킹 그리고 다른 물리적 기기, 하부 구조 그리고 온갖 유형의 전자 데이터를 만들고, 처리하며, 저장하고, 확보하며 교환하는 과정이 포함됩니다.

ID	기준	시행 안내	필수/권장
4.1	CTPAT 회원은 정보 기술(IT)을 보호하기 위한 목적의 문서로 된 종합적인 사이버 보안 정책 그리고/또는 절차를 갖추고 있어야 합니다. 문서로 된 IT 정책은 최소한 모든 개인 사이버 보안 기준을 다루어야 합니다.	인정된 산업 프레임워크/기준에 기초한 사이버 보안 규정을 따를 것을 회원에게 권장합니다. *국립 표준 기술원(NIST)은 국내와 외국의 사이버 보안 위험을 관리하고 완화하는 기존 기준, 지침 그리고 관행에 기초해 자발적인 지침을 제시하는 사이버 보안 프레임워크(https://www.nist.gov/cyberframework)를 제공하는 조직입니다. 프레임워크는 사이버 보안 위험을 줄이기 위한 행동을 파악하고 그 우선순위를 정하는 데 도움이 되며, 그런 위험을 관리하는 정책, 사업 그리고 기술적인 접근을 조정하는 도구입니다. 그것은 조직의 위험 관리 과정과 사이버 보안 프로그램을 보완해 줍니다. 아니면 기존 사이버 보안 프로그램을 갖추고 있지 않은 조직의 경우 이 프레임워크를 참고삼아 자체적 프로그램을 만들 수 있습니다. *NIST 는 측정 기준을 장려하고 유지하는 상무부 산하 비규제 연방 기관일 뿐만 아니라 연방 정부의 기술 기준 개발 기관입니다.	필수

ID	기준	시행 안내	필수/ 권장
4.2	흔한 사이버 보안 위협으로부터 정보 기술(IT)을 보호하기 위해 회사는 회원의 컴퓨터 시스템에 있는 멀웨어(바이러스, 스파이웨어, 웜, 트로얀 등)와 내부/외부 침투(방화벽)를 막는 소프트웨어/하드웨어를 설치해야 합니다. 회원은 자신의 보안 소프트웨어가 여전히 유효하며 정기적인 보안 업데이트를 받을 수 있게 해야 합니다. 회원은 사회 공학을 이용한 공격을 막기 위한 정책과 절차를 갖추고 있어야 합니다. 데이터 유출이 있거나 데이터 그리고/혹은 장비의 손실로 인해 예기치 못한 다른 사건이 생긴 경우, IT 시스템 그리고/또는 데이터 복구(혹은 교체) 작업이 절차에 포함되어야 합니다.		필수

ID	기준	시행 안내	필수/ 권장
4.3	CTPAT 회원은 네트워크 시스템을 이용해 자신의 IT 하부구조의 보안성을 정규적으로 검사해야 합니다. 취약점이 발견되면 현실적으로 가장 빠른 시점에 시정 조치를 해야 합니다.	보안이 유지된 컴퓨터 네트워크는 사업에 가장 중요한 부분이며, 확실한 보호를 위해서는 정규적인 검사가 필요합니다. 이것은 취약점 검사 일정을 잡는 식으로 할 수 있습니다. 사업장에서 보안 요원이 열려 있는 문과 창문을 점검하듯이 취약점 검사(VS)는 해커가 회사 IT 시스템에 접속할 수 있는 열린 공간이 운영 시스템이나 소프트웨어에 있는지(열린 포트와 IP 주소) 찾아냅니다. VS 는 검사 결과를 알려진 취약점 데이터와 비교하는 식으로 이 작업을 하며, 사업체가 행동에 옮길 시정 보고서를 발행합니다. 무료로 이용할 수 있는 상용 버전 취약점 검사기가 많이 있습니다. 검사의 빈도수는 회사의 사업 모델과 위험 수준과 같은 다양한 요인에 따라 달라집니다. 예를 들어 회사는 사업의 네트워크 하부구조가 바뀔 때마다 이런 검사를 해야 합니다. 그러나 사이버 공격이 모든 크기의 사업체에서 증가하고 있으므로, 검사 일정을 잡을 때는 이 점을 고려해야 합니다.	필수

ID	기준	시행 안내	필수/권장
4.4	사이버 보안 정책은 회원이 사이버 보안 위협에 대한 정보를 정부와 다른 사업 파트너와 어떻게 공유하는지를 다루어야 합니다.	회원이 사이버 보안 위협에 대한 정보를 정부와 공급망 내 다른 사업 파트너와 공유할 것을 권장합니다. 정보 공유는 악의적인 사이버 활동에 대한 상황 인식을 공유하고자 하는 국토안보부의 임무에서 중요한 부분입니다. CTPAT 회원은 "국립 사이버 위협 정보 통합 센터"(NCCIC - https://www.us-cert.gov/nccic)에 가입할 수 있습니다. NCCIC 는 취약점과 사건 그리고 완화에 대한 인식을 고취시키기 위해 정보를 공공 및 민간 부문과 공유합니다. 사이버 및 산업 규제 시스템 이용자는 정보 제품, 피드 그리고 서비스를 무료로 받아볼 수 있습니다	권장
4.5	직원과 하도급자가 내부 시스템과 외부 웹사이트를 부적절하게 접속하고 사업 데이터를 조작하거나 변경하는 것을 포함해 IT 시스템/데이터 무허가 접속 혹은 정책과 절차 위반을 찾아낼 수 있는 시스템이 있어야 합니다. 위반자는 모두 적절한 징계를 받아야 합니다.		필수
4.6	사이버 보안 정책과 절차는 매년 혹은 상황이나 위험으로 인해 필요한 경우 더 자주 검토되어야 합니다. 검토 후 정책과 절차는 필요한 경우 갱신되어야 합니다.	일 년이 지나기 전에 정책을 갱신해야 하는 상황의 한 예로 사이버 공격을 들 수 있습니다. 이 공격으로부터 배운 교훈은 회원의 사이버 보안 정책을 강화하는 데 도움이 될 것입니다.	필수

ID	기준	시행 안내	필수/ 권장
4.7	사용자 접속이 직무 기술이나 맡은 업무에 따라 제한되어야 합니다. 민감한 시스템 접속이 직무 요건에 기초하도록 허가된 접속을 정기적으로 검토해야 합니다. 직원이 회사를 그만두면 컴퓨터와 네트워크 접속을 하지 못 하게 해야 합니다.		필수

ID	기준	시행 안내	필수/권장
4.8	정보 기술(IT) 시스템에 접속할 수 있는 개인은 개적으로 지정된 계정을 사용해야 합니다. IT 시스템 접속은 강력한 암호, 암호구 혹은 다른 인증 양식의 사용을 통해 침투를 막아야 하며, IT 시스템의 사용자 접속을 보호해야 합니다. 암호 그리고/또는 암호구는 침해 증거가 있거나 침해되었다는 합리적인 의심이 드는 즉시 변경해야 합니다.	IT 시스템 침해를 막으려면 인증 과정을 거쳐 사용자 접속을 보호해야 합니다. 세 가지 다른 방식의 인증 과정으로 복잡한 암호나 암호구, 생체 인식 기술 그리고 전자 신분 카드를 들 수 있습니다. 두 가지 이상을 사용하는 과정이 낫습니다. 이것을 이중 인증(2FA) 혹은 다중 인증(MFA)이라고 합니다. 로그온 과정에서 사용자가 세 가지 이상의 증명(크리덴셜)을 제시해야 하므로 MFA 가 가장 안전합니다. 약한 암호나 크리덴셜 절도를 통해 이루어진 네트워크 침입을 종료하는 데 MFA 가 도움이 됩니다. 개인이 (자신이 이미 알고 있는) 암호나 암호구를 토큰이나 자신의 물리적 특징(생체) 중 하나로 보강하도록 해서 이런 공격 요인을 차단하는 데 MFA 가 도움이 됩니다. 암호를 사용하는 경우 복잡한 암호를 사용해야 합니다. 국립표준기술원(NIST)의 특별 간행물 800-63B: 디지털 정체성 지침 (https://pages.nist.gov/800-63-3/sp800-63b.html)은 암호 지침을 포함합니다. 이 지침은 단어와 특수 문자보다는 길고 기억하기 쉬운 암호구를 권장합니다. 이런 긴 암호구(NIST 는 최대 길이 64 자를 권장)는 쉽게 기억할 수 있는 단어나 어휘의 조합이기 때문에 해독하기가 훨씬 더 어렵습니다.	필수

ID	기준	시행 안내	필수/권장
4.9	사용자가 네트워크에 원격 접속을 하도록 허용하는 회원은 가상사설망(VPN)과 같은 보안 기술을 사용해 직원이 회사 외부에 있을 때 회사의 인트라넷을 안전하게 접속할 수 있게 해야 합니다. 회원은 또한 승인되지 않은 사용자가 원격 접속을 하지 못 하도록 절차를 설계해야 합니다.	VPN 외에 다른 방식으로도 원격 접속을 보호할 수 있습니다. 다중 승인(MFA)이 그 다른 방식입니다. 다중 승인의 예로 직원이 네트워크에 접속하기 위해 입력해야 하는 동적 보안 코드가 들어 있는 토큰을 들 수 있습니다.	필수
4.10	직원이 개인 기기로 회사 일을 하는 것을 허용하는 회원의 경우, 그런 모든 기기가 정기적인 보안 갱신과 안전하게 회사의 네트워크를 접속하는 방법이 포함된 회사의 사이버 보안 정책과 절차를 준수해야 합니다.	개인 기기에는 CD, DVD 그리고 USB 플래시 드라이브 같은 저장 매체가 포함됩니다. 직원이 개인 매체로 개별 시스템에 연결하는 것을 허용할 때는 조심할 필요가 있는데, 그것은 이런 데이터 저장 기기가 회사 네트워크 사용으로 전파될 수 있는 멀웨어에 감염될 수 있기 때문입니다.	필수

ID	기준	시행 안내	필수/ 권장
4.11	사이버 보안 정책과 절차에는 위조 혹은 비정상적인 허가를 받은 기술 제품의 사용을 막는 방법이 포함되어야 합니다.	컴퓨터 소프트웨어는 그것을 만든 조직이 소유하는 지식 재산(IP)입니다. 제조자나 발행자의 명시적 허락이 없으면 어떻게 구했는가에 상관없이 소프트웨어를 설치하는 것은 불법입니다. 허락은 거의 매번 승인된 소프트웨어 사본과 함께 발행자가 허가하는 양식입니다. 무허가 소프트웨어는 업데이트를 할 수 없기 때문에 작동하지 않을 가능성이 큽니다. 그것은 멀웨어가 들어 있기가 쉬워 컴퓨터와 정보를 무용지물로 만듭니다. 무허가 소프트웨어에 대한 보증이나 지원을 기대할 수 없기 때문에 고장이 나면 귀하의 회사가 알아서 해결해야 합니다. 막대한 민사 벌금과 형사 처벌과 같이 무허가 소프트웨어는 법적인 결과도 초래합니다. 소프트웨어 해적 행위는 합법적이고 승인된 소프트웨어의 가격을 높이게 되고 새로운 소프트웨어 연구 개발에 쓸 수 있는 자금을 줄이게 됩니다. 회원은 새로운 매체를 구입할 때 제품 키 라벨과 진품 증서를 보관하고 있어야 한다는 정책을 만들 수 있습니다. CD, DVD 그리고 USB 매체에는 소비자가 진품을 받고 위조를 막기 위해 홀로그램 보안 기능이 포함되어 있습니다.	권장

ID	기준	시행 안내	필수/권장
4.12	데이터는 일주일에 한번 혹은 필요한 경우 백업이 되어야 합니다. 민감한 기밀 데이터는 암호화된 포맷으로 저장되어야 합니다.	데이터 상실로 조직 내 개인이 받는 타격이 다를 수 있으므로 데이터 백업을 해 두어야 합니다. 생산이나 공유 서버가 침입을 받거나 데이터를 상실하는 것에 대비해 매일 백업을 하는 것을 또한 권장합니다. 개인 시스템의 경우 어떤 유형의 정보인가에 따라 백업을 그렇게 자주 할 필요가 없을 수도 있습니다. 백업 저장에 사용된 미디어는 외곽 시설에 저장하는 것이 좋습니다. 데이터 백업에 사용된 기기를 생산 작업을 한 네트워크와 같은 네트워크에서 사용해서는 안 됩니다. 클라우드에 데이터를 백업하는 것은 "오프 사이트" 시설에서 하는 것이 허용됩니다.	권장
4.13	수입/수출 과정에 관한 민감한 정보를 담고 있는 모든 매체, 하드웨어 혹은 다른 IT 장비는 정기 재고 조사를 통해 그 수를 확인해야 합니다. 그것을 폐기할 때는 국립표준기술원(NIST)의 매체 완전 삭제 지침이나 다른 적절한 산업 내 지침에 따라 적절하게 완전히 삭제하고/삭제하거나 폐기해야 합니다.	컴퓨터 미디어의 유형의 예로 하드 드라이브, 이동식 드라이브, CD-ROM 이나 CD-R 디스크, DVD 혹은 USB 드라이브를 들 수 있습니다. 국립표준기술원(NIST)은 정부의 데이터 매체 폐기 기준을 만들었습니다. 회원은 NIST 의 IT 장비 및 매체의 삭제·폐기 기준을 참고할 수 있습니다. 매체 완전 삭제: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	필수

두 번째 집중 영역: 교통 보안

5. <u>수송차와 국제 교역 도구 보안</u> – 밀수 계획에는 수송차와 국제 교역 도구(IIT)를 수정하거나 IIT 내부에 밀수품을 숨기는 것이 흔히 포함됩니다. 이 기준 유형은 무허가 물품이나 사람을 반입할 수 있게 하는 IIT 구조 변경이나 도구 내 은밀한 침입을 방지하고, 찾아내고/찾아내거나 저지하기 위한 보안 조치를 다루고 있습니다.

적입/적재 시 IIT 를 검사하고 적절하게 봉인하는 절차가 실시되어야 합니다. 수송 중이나 "휴지" 중인 화물은 통제를 적게 받기 때문에 침입에 더 취약한데, 바로 이런 이유로 수송 중인 화물/수송차를 추적하는 봉인 규제와 방법이 주요 보안 기준이 됩니다.

공급망 위반 행위가 수송 과정에서 가장 빈번하게 일어나므로 회원은 공급망 전체에 걸쳐 방심하지 말고 주요 화물 기준을 적용해야 합니다.

주요 정의: 국제 교역 도구 (IIT) – IIT 에는 컨테이너, 평상형 트럭, 단위탑재용기(ULD), 리프트밴, 화물밴, 선적 탱크, 통, 스키드, 화물 운반대, 카울 보드, 의류 원단 심 혹은 국제 교역에서 상품을 수송하고 있거나 수송하기 위해 (적재되거나 빈 채로) 도착하는 다른 특수 컨테이너가 포함됩니다.

ID	기준	시행 안내	필수/권장
5.1	수송차와 국제 교역 도구(IIT)는 국제 교역 도구의 구조 변경이나 (해당 시) 봉인/문을 통한 침입의 결과를 초래할 수 있는 무허가 접근을 방지하기 위해 안전한 지역에 보관해야 합니다.	(비어 있건 꽉 차 있건) 수송차와 국제 교역 도구를 안전하게 보관하는 것은 무허가 접근을 막는 데 있어 중요합니다.	필수

ID	기준	시행 안내	필수/권장
5.2	CTPAT 검사 과정은 문서화된 보안 검사와 농업 검사를 위한 절차를 갖추고 있어야 합니다	수송차나 국제 교역 도구의 수정이 포함된 밀수 계획이 유행하고 있으므로 회원은 눈에 띄는 해충과 심각한 구조 결함을 찾아내기 위해 수송차와 국제 교역 도구 검사를 반드시 해야 합니다. 그런 의미에서 수송차와 IIT 를 통한 해충 오염을 방지하기 위해 농업 부분이 보안 검사 과정에 추가되었습니다. 해충 오염은 눈에 보이는 동물, 곤충 혹은 다른 무척추 동물(산 것 죽은 것 모두, 난낭과 난주를 포함해 모든 생활 주기) 혹은 모든 동물성 유기물(혈액, 뼈, 머리, 살, 분비물, 배설물 포함), 살릴 수 있거나 살릴 수 없는 식물이나 식물 제품(과일, 씨, 잎, 잔가지, 뿌리, 껍질 포함) 혹은 곰팡이와 같은 다른 유기물 또는 흙이나 물로서 국제 교역 도구(즉, 컨테이너, 단위탑재용기 등)의 적하 목록 화물이 아닌 제품으로 정의됩니다.	필수
5.3	CTPAT 회원은 다음과 같은 CTPAT 보안 및 농업 검사를 반드시 실시해야 합니다. 이런 검사 요건은 공급망이 육상에 기초하는지(캐나다나 멕시코) 혹은 공급망이 해외에서(바다나 항공 형태로) 기원했는가에 따라 달라집니다. 적입/포장 전에 빈 국제 교역 도구(IIT)는 모두 검사되어야 하며, 수송차 역시 육상 국경을 넘어 미국에 들어올 때 검사가 되어야 합니다. <u>해상, 하늘, 육지 국경을 통한 선로 혹은 협동일관 화물에 의한 CTPAT 선적에 대한 검사 요건:</u>	밀수품을 숨기기 위해 구조를 수정하거나 눈에 보이는 농업 해충으로 오염되었는지를 확인하기 위해 수송차와 국제 교역 도구(IIT)에 대해 보안 및 농업 검사가 이루어집니다. 해외 공급망의 경우 모든 IIT 도구에 대해 적입/포장 시 검사를 하게 되어 있습니다. 그러나 해양/항공을 통한 공급망이 더 높은 위험을 지닌 경우, 수송차가 포함된 더 포괄적인 검사 절차 그리고/또는 해상 터미널이나 항공 물류 시설에서의 검사가 필요할 수 있습니다. 보통 육상	필수

ID	기준	시행 안내	필수/권장
	모든 빈 컨테이너와 단위탑재용기(ULD)에 대해서는 일곱 군데 검사를 하고, 모든 빈 냉장 컨테이너와 ULD 에 대해서는 여덟 군데 검사를 해야 합니다. 1. 앞 벽 2. 왼쪽 3. 오른쪽 4. 바닥 5. 천장/지붕 6. 문 잠그는 장치의 보안성을 포함해서 문 안/바깥 7. 화물 운반칸 바깥/밑 8. 냉장 컨테이너의 팬 하우징 <u>고속도로 운송 회사를 통한 육지 국경 통과 시 추가 검사 요건:</u> 수송차와 IIT 검사는 수송차/IIT 보관 야적장에서 해야 합니다. 가능하면 보관 야적장을 들어오고 나갈 때 그리고 적재/적입 시점에 검사를 해야 합니다. 이런 체계적인 검사에는 다음의 17 가지 검사가 포함되어야 합니다. **<u>트랙터:</u>**	국경을 통과하는 선적이 위험 수준이 높은데, 그런 이유로 수송차와 IIT 둘 다 여러 차례 검사를 받게 됩니다. 다양한 형식의 II 의 예로 해양 컨테이너, 냉장 컨테이너/트레일러, 장거리 트레일러, 탱크 컨테이너, 레일/유개차, 호퍼 그리고 단위탑재용기(ULD)를 들 수 있습니다. CTPAT 포털의 공공 도서관 섹션에서 보안과 농업 수송차/국제 교역 도구 검사에 대한 교육 자료를 찾을 수 있습니다.	

ID	기준	시행 안내	필수/권장
	1. 범퍼/타이어/림 2. 문/도구 칸 그리고 잠금 장치 3. 배터리 상자 4. 에어 브리더 5. 연료 탱크 6. 내부 운전 칸/침대칸 7. 페어링지붕 **트레일러**: 1. 다섯 번째 바퀴 부분 – 원래 있는 칸/스키드 플레이트 점검; 2. 외부 – 앞/옆 3. 뒤 – 범퍼/문 4. 앞 벽 5. 왼쪽 6. 오른쪽 7. 바닥 8. 천장/지붕 9. 문 잠그는 장치의 보안성을 포함해서 문 안/바깥 10. 화물 운반칸 바깥/밑		

ID	기준	시행 안내	필수/권장
5.4	수송차와 국제 교역 도구는 (필요한 경우) 그것을 제거하려는 시도를 어느 정도 견딜 수 있는 외부 하드웨어를 갖추고 있어야 합니다. 문, 손잡이, 로드, 걸쇠, 리벳, 브래킷 그리고 컨테이너 문 잠금 장치 모든 다른 부분은 봉인 기기를 부착하기 전에 조작이나 하드웨어 불일치가 없는지 확인하기 위해 모두 검사를 해야 합니다.	조작 방지 경첩이 달린 컨테이너/트레일러를 이용하는 것을 고려하십시오. 또한, 회원은 보호 플레이트나 핀을 최소한 문 경첩 두 개에 두고/두거나 점착성 봉인/테이프를 한 쪽마다 적어도 한 경첩에 붙일 수 있습니다.	필수
5.5	모든 수송차와 국제 교역 도구 검사는 점검 목록에 들어 있어야 합니다. 점검 목록에 다음과 같은 사항이 들어 있어야 합니다. • 컨테이너/트레일러/국제 교역 도구 번호 • 검사 날짜 • 검사 시간 • 검사를 하는 직원의 이름 • 검사를 한 구체적인 국제 교역 도구 부분 검사를 감독하는 경우 감독은 또한 점검 목록에 서명을 해야 합니다. 작성된 컨테이너/국제 교역 도구 검사 종이가 선적 문서 패킷의 일부로 들어가야 합니다. 수하인은 상품을 받기 전에 작성된 선적 문서 패킷을 받아야 합니다.		권장
5.6	모든 보안 검사는 접속이 통제되고 가능하면 CCTV 시스템을 통해 모니터링이 되는 장소에서 이루어져야 합니다.		권장

ID	기준	시행 안내	필수/권장
5.7	눈에 보이는 해충 오염이 수송차/국제 교역 도구(IIT) 검사 시 발견되면, 그런 오염을 제거하기 위해 세탁/진공 청소를 해야 합니다. 이런 검사 요건을 준수한다는 것을 보여주기 위해 문서 기록을 일 년간 보관하고 있어야 합니다.	발견된 오염 물질의 종류, 오염 물질이 발견된 장소(수송차 장소) 그리고 해충 오염이 어떻게 제거되었는가를 기록하는 것은 회원의 미래 해충 오염 예방에 도움이 될 수 있는 유용한 행위입니다.	필수
5.8	위험 정도에 따라서 관리 직원은 운송 직원이 수송차/국제 교역 도구 검사를 끝낸 뒤 무작위 검색을 해야 합니다. 수송차 검색은 위험에 따라 빈도수를 높이면서 정기적으로 실시해야 합니다. 검색은 예상할 수 없도록 경고 없이 무작위로 실시되어야 합니다. 운송 회사 야적장, 트럭이 적재된 후 그리고 미국 국경으로 가는 중간과 같이 수송차가 침입을 받기 쉬운 여러 장소에서 검사를 해야 합니다.	수송차 감독 수색은 내부 음모를 막기 위해 합니다. 감독이 물건 하나(장난감이나 색깔이 있는 상자)를 수송차 속에 숨겨 현장 검사관/수송 운영관이 그것을 찾아내는지 알아보는 것은 최상의 관행이라 할 수 있습니다. 보안에 대해 상급 관리자에게 보고를 하는 보안 책임자나 다른 지정된 관리 직원이 감독 직원이 될 수 있습니다.	권장
5.14	CTPAT 회원은 원지점에서 최종 목적지까지 수송차를 추적하기 위해 수송 제공자와 협력해 일해야 합니다. 추적, 보고 그리고 데이터 공유에 대한 구체적인 요건이 서비스 제공자와의 서비스 계약서 조건 내에 포함되어야 합니다.		권장
5.15	송하인은 자신의 선적 이동을 추적할 수 있도록 운송 회사의 GPS 차량 모니터링 시스템에 접속할 수 있어야 합니다.		권장
5.16	미국 국경 근처에 있는 육상 국경 선적의 경우 예정에 없는 정지에 대해 "무정지" 정책이 적용되어야 합니다.	휴지 중인 화물은 위험에 노출되어 있습니다. 예정된 정지는 이 정책에서 다루지 않지만, 전체 추적 및 모니터링 절차에서 다뤄져야 합니다.	권장

ID	기준	시행 안내	필수/권장
5.24	고위험 지역에서는 국경 통과 직전에 CTPAT 회원은 미국행 선적이 수송차/국제 교역 도구가 조작된 흔적을 찾아내는 "마지막" 확인 과정에 수송차 육안 검사와 VVTT 봉인 확인 과정을 포함해야 합니다. 검사는 적절한 교육을 사람이 해야 합니다. V – 봉인과 컨테이너 잠금 장치를 본다. 그것이 제대로 되어 있는 것을 확인한다. V – 봉인 번호가 정확한지 확인하기 위해 선적 문서와 비교한다. T – 봉인이 제대로 부착되어 있는지 확인하기 위해 봉인을 잡아당겨 본다. T – 부분이 열리고 서로 분리되거나 봉인 중 한 부분이 헐거워지지 않도록 볼트 봉인을 비틀고 돌려 본다.		권장
5.29	신빙성이 가는(혹은 포착된) 선적이나 수송차의 보안 위협이 발견된 경우 회원은 (현실적으로 가능한 빨리) 영향을 받을 수 있는 모든 사업 파트너와 필요한 경우 법 집행 기관에 알려야 합니다.		필수

6. <u>봉인 보안</u> – 트레일러와 컨테이너 봉인은 봉인이 온전하게 계속 유지되게 하기 위해 계속 안전한 공급망의 중요한 요소가 됩니다. 봉인 보안에는 포함됩니다. 봉인 보안에는 각 CTPAT 요건에 따라 올바른 봉인을 사용하고 IIT 에 봉인을 제대로 하며 봉인이 제대로 부착되었는지 확인하는 것처럼 봉인 보안의 모든 측면을 다루는 종합적인 봉인 정책이 포함되어 있습니다.

ID	기준	시행 안내	필수/권장
6.1	CTPAT 회원은 봉인이 어떻게 발행되며 시설과 운송 중에 통제가 되는지를 기술하는 문서로 된 상세한 높은 보안 봉인 절차를 갖추고 있어야 합니다. 절차는 문서로 된 사건 기록, 파트너에 대한 의사소통 규정 그리고 사건의 조사를 포함해 봉인이 변경되고 조작되거나 틀린 봉인 번호를 가지고 있는 경우 취할 조치 단계를 설명해야 합니다. 검사를 통해 찾아낸 사항은 반드시 문서 기록이 되어야 하며, 되도록 가능한 한 빨리 시정 조치가 이루어져야 합니다. 이러 문서화된 절차는 접근이 용이하도록 지역 운영 수준에서 유지되어야 합니다. 절차는 필요한 경우 갱신하고 적어도 일 년에 한 번씩 검토해야 합니다. 문서로 된 봉인 관리는 다음과 같은 요소를 포함하고 있어야 합니다. **봉인 접근 관리**:		필수

ID	기준	시행 안내	필수/권장
	• 봉인 관리를 승인된 직원에게만 허용해야 합니다. • 보관 장소를 안전하게 유지하십시오. **재고 조사, 배포 및 추적(봉인 일지):** • 새로 받은 봉인 기록 • 일지에 기록된 봉인 발행 • 일지를 통해 봉인 추적 •교육과 승인을 받은 직원만이 봉인을 국제 교역 도구(IIT)에 부착할 수 있음 **운송 중 봉인 관리**: • 봉인이 된 IIT 를 수거해올 때(혹은 정지 후에) 봉인에 조작 흔적이 없는지 확인합니다. • 봉인 번호가 선적 문서에 기록된 것과 일치하는지 확인합니다. **운송 중 깨진 봉인:** •적재물을 검사하는 경우, 교체 봉인 번호를 기록합니다. • 봉인이 깨지면 운전기사는 즉시 파견 업체에 통보해 누가 봉인을 깨뜨렸는지 알려주고 새로운 봉인 번호를 제공해야 합니다. • 운송 회사는 송하인과 브로커 그리고 수입업자에게 봉인 변경과 봉인 번호 교체를 즉각 통보해야 합니다. • 송하인은 봉인 일지에 교체 봉인 번호를 기록해야 합니다.		

ID	기준	시행 안내	필수/권장
	봉인 불일치: • 조사에 협조하기 위해 변경되거나 조작된 봉인을 보관합니다. •불일치를 조사하고 (필요한 경우) 시정 조치를 했는지 확인합니다. • 필요한 경우, 조사에 협조하기 위해 CBP 와 관련 외국 정부에 훼손된 봉인을 보고합니다.		
6.2	봉인할 수 있는 모든 CTPAT 선적은 책임 당사자(즉, 송하인이나 송하인을 대리해 행위하는 포장자) 적재/적입/포장 직후 높은 보안 봉인에 대한 가장 최근의 국제표준화기구(ISO) 17712 기준을 만족시키거나 넘어서는 높은 보안 봉인으로 보안이 되어야 합니다. 기준을 만족시키는 케이블 및 볼트 봉인 둘 다 허용이 됩니다. 모든 봉인은 CTPAT 회원의 화물을 미국으로/으로부터 운송하는 국제 교역 도구에 제대로 안전하게 부착되어야 합니다.	사용하는 높은 보안 봉인은 가능하면 오른쪽 문 손잡이 보다는 안전한 캠포지션에 위치하게 해야 합니다. 봉인은 오른쪽 컨테이너 문의 가장 수직인 바의 중간 바닥에 위치해야 합니다. 안전한 캠포지션이 가능하지 않은 경우 대안으로 오른쪽 컨테이너 문의 가장 왼쪽 잠금 손잡이 중간에 위치하게 할 수 있습니다. 볼트 봉인이 사용되는 경우, 볼트 봉인을 배럴 부분과 같이 두거나 걸쇠 위 배럴 부분과 함께 위로 보도록 끼워 넣을 것을 권합니다	필수
6.5	(봉인 재고 조사를 하는) CTPAT 회원은 자신이 사용하는 높은 보안 봉인이 가장 최근 ISO 17712 기준을 만족시키거나 넘어선다는 것을 문서로 기록해야 합니다.	ISO 높은 보안 봉인 기준을 준수했다는 것을 보여주는 연구소 검사 인증서는 준수 증거로 채택될 수 있습니다. CTPAT 회원은 구매하는 봉인에 조작한 흔적이 없는지를 알고 있어야 합니다.	필수

ID	기준	시행 안내	필수/권장
6.6	회원이 봉인의 재고를 유지하는 경우, 회사 경영진이나 보안 책임자는 보관된 봉인의 주기적인 재고 조사 그리고 재고 일지와 선적 문서 간의 일치 비교가 포함된 봉인 감사를 실시해야 합니다. 모든 감사는 문서 기록이 되어야 합니다. 부두 책임자 그리고/또는 창고 관리자는 전체 봉인 감사 과정의 일부로 수송차와 국제 교역 도구에 사용된 봉인 번호를 정기적으로 확인해야 합니다.		필수
6.7	CTPAT 의 봉인 확인 과정은 모든 높은 보안 봉인(볼트/케이블)이 국제 교역 도구에 제대로 부착이 되며 설계된 대로 작동되도록 진행되어야 합니다. 절차는 VVTT 과정으로 알려져 있습니다. V – 봉인과 컨테이너 잠금 장치를 본다. 그것이 제대로 되어 있는 것을 확인한다. V – 봉인 번호가 정확한지 확인하기 위해 선적 문서와 비교한다. T – 봉인이 제대로 부착되어 있는지 확인하기 위해 봉인을 잡아당겨 본다. T – 부분이 열리고 서로 분리되거나 봉인 중 한 부분이 헐거워지지 않도록 볼트 봉인을 비틀고 돌려 본다	케이블 봉인을 사용하는 경우, 봉인이 위나 아래로 움직이지 못 하도록 봉인이 수직 바의 직사각형 하드웨어 바닥을 둘러싸도록 해야 합니다. 봉인을 설치한 후 케이블 양편이 헐렁하지 않도록 하십시오. 케이블 봉인에 대한 VVTT 과정을 써서 케이블이 탱탱하도록 해야 합니다. 제대로 설치했으면 잠금 몸체 안에서 케이블이 미끄러질 수 있는지 확인하기 위해 케이블을 잡아당기고 끌어당겨 보십시오.	필수

7. <u>절차상 보안</u> – 절차상 보안은 수입-수출 과정, 문서화 그리고 화물 보관 및 취급 요건에 관련된 여러 측면을 포함하고 있습니다. 다른 중요한 절차적 기준은 사건 보고와 해당 법 집행국에 통보하는 것과 관련되어 있습니다. 뿐만 아니라 CTPAT 는 자주 절차를 문서로 기록할 것을 요구하는데, 그렇게 했을 때 시간이 지나면서 균일한 과정을 유지하는 데 도움이 되기 때문입니다. 그럼에도 불구하고 이런 문서로 된 절차에 필요한 세부 정보의 양은 사업 모델이나 그 절차에 의해 다루어진 내용과 같은 여러 요소에 따라 달라집니다.

공급망에 쓰인 기술이 계속해서 발전한다는 것을 CTPAT 는 알고 있습니다. 기준 전반에 걸쳐 쓰이는 용어는 문서로 된 절차, 문서 그리고 양식에 기초하지만 그렇다고 이 문서가 종이 문서일 필요는 없습니다. 전자 문서, 서명 그리고 다른 디지털 기술도 이런 방식을 만족시킨다고 할 수 있습니다.

프로그램은 "동일한" 양식으로 설계된 것이 아닙니다. 그러므로 각 회사가 (자체 위험 평가에 기초하여) 절차를 어떻게 실시하고 유지할지 결정해야 합니다. 그러나 보안 규정에 대한 설명서를 따로 만드는 것보다는 기존 절차 내에 보안 절차를 포함하는 것이 더 효과적입니다. 이것이 더 지속가능한 구조를 만들고 공급망 보안이 모든 이의 책임이라는 사실을 강조하는 데 일조를 하게 됩니다.

ID	기준	시행 안내	필수/ 권장
7.1	화물이 밤새 혹은 장시간 대기하고 있는 경우, 화물에 대한 무허가 접근을 막기 위한 조치를 취해야 합니다.		필수
7.2	화물 중간 대기 구역과 인접 지역은 눈에 보이는 해충 오염이 없도록 정기적으로 검사를 해야 합니다.	필요한 경우, 미끼, 올가미 혹은 다른 장애물을 예방책으로 사용할 수 있습니다. 잡초 제거나 무성한 식물을 줄이는 것이 중간 대기 구역 내 해충 서식을 제거하는 데 도움이 됩니다	필수

ID	기준	시행 안내	필수/권장
7.4	화물을 컨테이너/IIT 에 적재/적입할 때는 보안 책임자/관리자 혹은 다른 지정된 직원이 감독을 해야 합니다.		권장
7.5	봉인을 제대로 설치했다는 것을 문서 증거로 남기기 위해 디지털 사진을 적입 시 찍어야 합니다. 현실적으로 가능하면 이런 이미지가 확인 목적으로 목적지에 전달되어야 합니다.	화물 표시, 적재 과정, 봉인이 붙여진 장소 그리고 제대로 설치된 봉인에 대한 증거를 문서화하기 위해 찍은 사진이 사진 증거에 포함됩니다.	권장
7.6	상품/화물의 세관 통과에 사용된 모든 정보가 판독이 가능하고, 완전하며, 정확하며, 교환이나 상실 혹은 잘못된 정보의 도입을 막고, 제때 보고가 되도록 확인하는 절차가 있어야 합니다.		필수
7.7	종이 문서가 사용되는 경우, 양식과 다른 수입/수출 관련 문서가 무허가로 사용되지 않도록 안전을 기해야 합니다.	잠글 수 있는 파일 캐비닛과 같은 방법을 사용해 적하 목록을 포함해 미사용된 양식이 무허가로 사용되지 않도록 안전하게 보관해야 합니다.	권장
7.8	송하인과 그 대리인은 선하증권(BOL) 그리고/또는 적하 목록이 운송 회사에 제공된 정보를 정확히 반영하는지 확인해야 하며, 운송 회사는 실사를 통해 이런 문서가 정확하다는 것을 확인해야 합니다. BOL 과 적하 목록은 미국 관세국경보호청(CBP)에 제 때 제출해야 합니다. CBP 에 제출한 BOL 정보는 미국이 목적지인 화물을 운송 회사가 처음으로 입수한 첫 번째 외국 장소/시설을 보여주어야 합니다. 무게와 개수가 정확해야 합니다.	봉인된 국제 교역 도구를 수거해 올 때 운송 회사는 송하인의 선적 지침에 나오는 정보에 의존할 수 있습니다. 봉인 번호을 선하증권(BOL)이나 다른 수출 문서에 전자로 인쇄해 달라고 요구하는 것은 봉인을 변경하거나 새로운 봉인 번호에 맞추려고 관련 문서를 변경하는 것을 막는 데 도움이 됩니다. 그러나 일부 공급망의 경우 상품이 운송 중에 외국 세관	필수

ID	기준	시행 안내	필수/ 권장
		당국이나 CBP 에 의해 검사될 수 있습니다. 정부에 의해 봉인이 깨지면 검사 후 주어진 새로운 봉인 번호를 기록하는 과정이 필요합니다. 어떤 경우에는 이것을 수기로 할 수도 있습니다.	

ID	기준	시행 안내	필수/권장
7.23	CTPAT 회원은 시설의 내부 보고 과정에 대한 기술이 포함된 사건 보고에 대해 문서로 된 절차를 갖추고 있어야 합니다. 전 세계 어디에서나 발생하면서 회원의 공급망 보안에 영향을 줄 수 있는 모든 수상한 활동이나 보안 사고(예를 들어 마약 압수, 밀입국자 발견 등)를 보고할 수 있는 통지 규정이 있어야 합니다. 필요한 경우 회원은 모든 국제 사건을 자체 공급망 전문가, 가장 가까운 통관항, 해당 법집행기관 그리고 영향을 받은 공급망 일부일 수 있는 사업 파트너에게 보고해야 합니다. CBP 에 하는 통지가 현실적으로 가장 빠른 시점이나 수송차나 IIT 가 국경을 통과하기 전에 이루어져야 합니다. 통지 절차에는 통지를 해야 하는 직원뿐만 아니라 법 집행기관의 이름과 전화번호 목록이 들어간 정확한 연락 정보가 포함되어 있어야 합니다. 연락 정보가 정확한지 확인하기 위해 절차를 정기적으로 검토해야 합니다.	미국 관세국경보호청에 반드시 통지를 해야 하는 사건은 다음을 포함합니다(다음에 국한되지는 않음). • 컨테이너/IIT 나 높은 보안 봉인 조작 • 수송차나 IIT 에 숨겨진 칸 발견 •기록되지 않은 새로운 봉인이 IIT 에 적용되었음. • 사람을 포함한 밀수품의 밀반입, 밀입국자 •수송차, 기관차, 선박 혹은 항공 운송기에 무허가 선적 • 강탈, 보호에 대한 지불, 위협 그리고/또는 협박 •사업체 식별기 [즉, 수입업자(IOR)의 납세 번호, 표준 운송인 알파벳(SCAC) 코드 등]의 무허가 사용	필수
7.24	무허가/무확인 개인을 파악하고, 검문하며, 처리하는 절차가 있어야 합니다. 알려지지 않거나 허가받지 않은 사람을 검문하고, 그런 상황에 어떻게 대처하며, 허가를 받지 않은 사람을 부지에서 내보내는 절차에 대한 규정을 직원은 알고 있어야 합니다.		필수

ID	기준	시행 안내	필수/권장
7.25	CTPAT 회원은 보안 관련 문제를 익명으로 신고할 수 있는 구조를 확립해야 합니다. 혐의가 접수되면 그것을 조사하고 필요한 경우 시정 조치를 취해야 합니다.	절도, 사기 그리고 내부 음모와 같은 내부 문제는 신고 당사자가 우려 사항을 익명으로 신고할 수 있다는 점을 알고 있는 경우에 더 용이하게 신고가 접수될 수 있습니다. 사람들이 자신의 행동에 대한 보복을 두려워하는 경우, 익명으로 신고있을 수 있는 핫라인 프로그램이나 이와 비슷한 제도를 회원은 마련할 수 있습니다. 모든 신고된 사안을 조사하고 시정 조치를 취했다는 사실을 문서로 남기기 위해 모든 신고 문서를 증거로 보관할 것을 권장합니다.	권장
7.27	부족, 초과 그리고 다른 중요한 불일치나 비정상의 경우는 모두 조사를 하고 필요한 경우에 해결이 되어야 합니다.		필수
7.28	도착하는 화물은 화물 적하 목록에 나오는 정보와 일치해야 됩니다. 떠나는 화물은 구매 혹은 배달된 주문과 일치하는지 확인해야 합니다.		권장
7.29	구체적인 선적에 지정된 봉인 번호는 출발 전에 수하인에게 전달되어야 합니다.		권장
7.30	봉인 번호는 선하증권 혹은 다른 선적 문서에 전자로 인쇄가 되어야 합니다.		권장
7.37	중대한 보안 사건이 발행한 이후, 회원은 해당 보안 관련 사건을 알게 된 즉시 그리고 공급망이 취약해졌는지 알기 위해서 후속 사건 분석을 실시해야 합니다. 이러한 분석은 정부 법 집행 기관에 의해 이미 실시된 것으로 알려진 조사를	보안 사건은 보안 조치가 회피, 생략 혹은 위반되었고, 형사적 처벌을 초래하였거나 초래할 수 있는 위반 행위입니다. 보안 사건은 테러 행위, 밀반입(마약, 사람 등) 및 밀항자 존재 여부를 포함합니다.	필수

ID	기준	시행 안내	필수/ 권장
	지연하거나 방해해서는 안 됩니다. 회사의 후속 사건 분석 결과는 문서로 기록을 하고, 되도록 신속히 끝내야 하며, 법 집행 기관에 의해 허용되는 경우 공급망 보안 전문가(SCSS)에 제공되어야 합니다.		

8. <u>농업 보안</u> – 농업은 미국에서 가장 큰 산업이며 고용 부문입니다. 또한, 농업은 침입적이고 파괴적인 해충과 질병을 품고 있을 수 있는 흙, 동물 배설물, 씨앗, 동·식물 재료와 같은 외국 동물 및 식물 오염물의 유입으로 인해 위협을 받는 산업이기도 합니다. 수송차와 모든 유형의 화물에서 오염 물질을 제거하면 CBP 화물 보관, 지연 그리고 상품 반환이나 처리를 줄일 수 있습니다. CTPAT 의 농업 요건을 확실히 준수하는 것은 또한 미국의 주요 산업과 전반적인 세계 식량 공급을 보호하는 데 도움이 됩니다.

주요 정의: 해충 오염 – 국제해상기구는 해충 오염을 눈에 보이는 동물, 곤충 혹은 다른 무척추 동물(산 것 죽은 것 모두, 난낭과 난주를 포함해 모든 생활 주기) 혹은 모든 동물성 유기물(혈액, 뼈, 머리, 살, 분비물, 배설물 포함), 생존 가능하거나 생존이 불가능한 식물이나 식물 제품(과일, 씨, 잎, 잔가지, 뿌리, 껍질 포함) 혹은 곰팡이와 같은 다른 유기물, 흙이나 물로서 국제 교역 도구(즉, 컨테이너, 단위탑재용기 등)의 적하 목록 화물이 아닌 제품으로 정의합니다.

ID	기준	시행 안내	필수/권장
8.1	CTPAT 회원은 목재포장제(WPM) 규정을 준수를 포함해 눈에 보이는 해충 오염을 방지하는 목적의 문서화된 절차를 사업 모델에 기초해 갖추고 있어야 합니다. 눈에 보이는 해충 오염 방지 조치를 공급망 전체에 걸쳐 취해야	WPM 은 상품을 지탱하고 보호하거나 운반하는 데 사용된 나무 혹은 나무 제품(종이 제품 제외)으로 정의됩니다. WPM 에는 화물 운반대, 대형 운반 상자, 상자, 릴 그리고 짐 깔개가 포함됩니다. 흔히 이런 물건은 해충을 제거하거나 죽이는 과정이나 처리를 충분히 거치지 않아 해충의 유입과 전파의 길목이 되는 원목으로 만들어집니다. 특히 짐 깔개는 해충의 유입과 전파 위험이 높은 것으로 드러났습니다. IPPC 는 해충과 오염원의 유입과 전파를 막고 통제하기 위해 조직화되고 효과적인 조치를 취하는 것을 목적으로 하는 국제 연합의 식량농업기구의 감독을 받는 다각적인 협정입니다. ISPM 15 에는 WPM 과 연관성이 있을 수 있는 해충의 유입과 전파 위험을 대폭 감소하기 위해	필수

ID	기준	시행 안내	필수/ 권장
	합니다. WPM 관련 조치는 국제식물보호협약(IPPC)의 식물위생 조치 국제 기준 15 호(ISPM 15)를 충족해야 합니다.	WPM 에 적용될 수 있는 국제적으로 수락된 조치가 포함되어 있습니다. ISPM 15 는 모든 목재 포장물에 적용되는데, 나무 껍질을 벗긴 뒤 열 처리를 하거나 브롬화메틸로 훈증하고 IPPC 준수 표시 도장이나 낙인을 찍도록 요구하고 있습니다. 이 준수 표시는 일상적으로 "밀 도장"(wheat stamp)으로 알려져 있습니다. 종이나 금속, 플라스틱이나 목판 제품(즉, 배향성 합판, 하드보드 그리고 합판) 같이 대체 재료로 만들어진 제품은 ISPM 15 에서 제외됩니다.	

세 번째 집중 영역: 사람 및 물리적 보안

9. 물리적 보안 –화물 처리 및 보관 시설, 국제 교역 도구 보관 장소, 국내 및 외국에 있는 수입/수출 문서가 작성되는 시설은 무허가 접근을 막는 물리적 장벽과 제지물을 갖추고 있어야 합니다.

CTPAT 의 초석 중 하나가 융통성이며 보안 프로그램은 각 회사의 상황에 맞게 만들어져야 합니다. 물리적 보안은 공급망 내 회원의 역할, 사업 모델 그리고 위험 수준에 따라 많이 달라질 수 있습니다. 물리적 보안 기준은 화물, 민감한 장비 그리고/또는 정보에 대한 무허가 접속을 막는 데 도움이 되는 여러 제지물/장애물을 제공하는데, 회원은 이런 보안 조치를 공급망 전체에 걸쳐 취해야 합니다.

ID	기준	시행 안내	필수/ 권장
9.1	트레일러 야적장과 사무실을 포함해 모든 화물 처리 및 보관 시설은 무허가 접근을 막는 물리적 장벽과 제지물을 갖추고 있어야 합니다.		필수

ID	기준	시행 안내	필수/권장
9.2	경계 울타리는 화물 처리 및 보관 시설 주위 영역을 둘러싸고 있어야 합니다. 시설이 화물을 처리하는 경우, 내부 울타리를 사용해 화물과 화물 처리 영역을 보호해야 합니다. 위험 정도에 따라 추가 내부 울타리를 통해 다양한 유형의 화물을 국내, 국제, 높은 가치 그리고/혹은 위험한 물질 같은 식으로 분리해야 합니다. 울타리가 온전하고 손상되지 않았는지 지정된 직원이 정규적으로 검사를 해야 합니다. 울타리에 손상된 부분이 발견되면 되도록 빨리 수리를 해야 합니다.	울타리 대신에 분리벽 혹은 가파른 절벽이나 무성한 덤불처럼 침투가 불가능하거나 침투를 지연시키는 자연적인 구조와 같은 다른 허용되는 제지물을 이용할 수 있습니다.	권장
9.4	차량 그리고/또는 직원이 들어가거나 나가는 출입문(그리고 다른 출구 지점)은 사람이 지키고 있거나 모니터링이 되어야 합니다. 지역·노동법에 따라 사람과 차량을 수색할 수도 있습니다.	출입구의 수를 적절한 접속과 보안에 최소로 필요한 수로 제한할 것을 권합니다. 출입이 통제되지 않는 시설의 출입문이 다른 출입점이 됩니다.	필수
9.5	개인 민간 승용차를 화물 처리 및 보관 영역이나 수송차 근처에 주차하는 것을 금지해야 합니다.	울타리 그리고/또는 운영 영역 바깥 아니면 화물 처리 및 보관 영역에서 최소한 상당히 떨어진 곳에 주차 공간을 정하십시오.	권장
9.6	적절한 조명이 필요한 경우 다음의 공간을 포함한 시설 내부와 외부에 공급되어야 합니다: 입구와 출구, 화물 처리 및 보관 영역, 울타리 선, 주차 공간.	적절한 보안 조명을 자동으로 켜는 자동 타이머나 광 센서가 조명 장치에 유용한 추가 장치가 될 수 있습니다.	필수

ID	기준	시행 안내	필수/권장
9.7	부지를 모니터링하고 민감한 영역의 무허가 접근을 막는 데 보안 기술이 사용되어야 합니다.	민감한 영역과 접속점을 보호하거나 모니터링하는 전자 보안 기술에는 다음이 포함됩니다: 침입탐지시스템(IDS)으로도 알려진 도난 경보 시스템(주위와 내부), 접속 통제 기기 그리고 폐쇄회로 텔레비전(CCTV)이 포함된 비디오 감시시스템. CCTV/VSS 시스템에는 아날로그 카메라(동축 사용), 인터넷 프로토콜(IP)을 사용하는 카메라(네트워크 사용), 녹화기 그리고 비디오 관리 소프트웨어가 포함됩니다. 비디오 감시가 도움이 될 수 있는 안전한/예민한 영역에는 다음이 포함됩니다: 화물 처리 및 보관 영역, 중요한 문서가 있는 선적/수령 영역, IT 서버, 국제 교역 도구(IT) 같은 것을 위한 야적장과 보관 영역, IIT 를 검사하는 영역, 봉인 보관 영역.	권장
9.8	물리적 보안을 위해 보안 기술에 의존하는 회원은 이 기술의 사용, 관리 그리고 보호를 주관하는 문서화된 정책과 절차를 갖추고 있어야 합니다. 최소한 다음과 같은 사항을 이런 정책과 절차가 규정하고 있어야 합니다. • 기술을 통제하고 관리하는 장소 출입이 허가된 사람으로 제한되어야 한다는 것 •정기적으로 기술을 테스트/검사할 때 사용된 절차	보안 기술이 제대로 작동하는지 확인하기 위해 정기적으로 테스트를 해야 합니다. 다음이 일반적으로 따라야 할 지침입니다. •서비스 작업 후 그리고 건물이나 시설의 주요 수리, 변경 혹은 추가 작업 동안 그리고 그 후에 보안 시스템을 테스트하십시오. 시스템 일부가 고의로 혹은 비고의적으로 손상을 입었을 수 있습니다. • 전화 혹은 인터넷 서비스에 큰 변경이 있은 후 보안 시스템을	필수

ID	기준	시행 안내	필수/권장
	• 모든 장비가 제대로 작동하며 필요한 경우 장비가 제대로 된 위치에 있다고 확인한 것이 검사에 포함되어 있다는 것 • 검사와 수행 테스트 결과가 문서로 기록됐다는 것 • 시정 조치가 필요한 경우 되도록 빨리 시정이 되어야 하며 시정 조치가 문서로 기록된다는 것 • 이런 검사의 문서화된 결과가 감사 목적으로 충분한 기간 보관된다는 것 삼자 중앙 모니터링 센터(외부)를 이용하는 경우 CTPAT 회원은 보안 코드 변경, 허가 직원 추가 및 제외, 암호 변경 그리고 시스템 접속 및 거부와 같은(여기에 국한되지는 않음) 중요한 시스템 기능과 인증 규정을 명기하는 문서화된 절차를 갖추고 있어야 합니다. 보안 기술 규정과 절차는 매년 혹은 위험 정도와 상황에 따라 필요하면 더 자주 검토와 갱신이 되어야 합니다.	테스트하십시오. 시스템이 모니터링 센터와 교신할 수 있는 능력에 영향을 줄 수 있는 것은 모두 재확인되어야 합니다. • 동작 인지 녹화, 동작 탐지 경보, 초당 이미지 그리고 품질 수준과 같은 비디오 세팅이 제대로 되었는지 확인하십시오. • 카메라 렌즈(혹은 카메라를 보호하는 돔)가 깨끗하며 렌즈의 초점이 잡히는지 확인하십시오. 가시성이 장애물이나 밝은 빛으로 인해 제한되어서는 안 됩니다. • 보안 카메라가 정확하게 위치되었고 제대로 된 위치를 계속 유지하는지 테스트를 하십시오(카메라가 인위적으로 혹은 실수로 움직여졌을 수 있습니다).	
9.9	보안 기술의 설계 및 설치를 고려할 때 CTPAT 회원은 허가/인증이 된 자원을 사용해야 합니다.	오늘날 보안 기술은 복잡하며 급속히 발전하고 있습니다. 회사들은 종종 필요한 때 효과가 없거나 필요 이상의 비용을 지불하는 식으로 잘못된 보안 기술을 구입합니다. 기준에	권장

ID	기준	시행 안내	필수/권장
		부합하는 지침을 따르면 구매자의 요구와 예산에 부합하는 기술을 선택하는 데 도움이 됩니다. 전국전기공사협회(NECA)에 따르면 현재 미국 33 개 주가 보안 및 경보 시스템 설치 작업에 종사하는 전문가가 충족해야 할 허가 요건을 두고 있습니다.	
9.10	모든 보안 기술 하부 구조는 무허가 접속으로부터 물리적으로 보호되어야 합니다.	보안 기술 하부 구조에는 컴퓨터, 보안 소프트웨어, 전자 컨트롤 패널, 비디오 감시 혹은 폐쇄 회로 텔레비전 카메라, 카메라의 전원 및 하드 드라이브 부품 뿐만 아니라 녹화물이 포함됩니다.	필수
9.11	보안 기술 시스템은 예기치 못한 직접 전력의 상실에 대비해 시스템이 계속 작동할 수 있게 하는 대체 전력원을 구비하고 있어야 합니다.	귀하의 보안망을 침입하려고 하는 범죄자가 보안망을 우회하기 위해 보안 기술 전원을 차단할 수 있습니다. 따라서 보안 기술의 대체 전력원을 마련해 두는 것이 중요합니다. 보조 발전원이나 예비 배터리가 대체 전력원이 될 수 있습니다. 예비 발전기는 또한 조명과 같은 다른 중요한 시스템에도 사용될 수 있습니다.	권장
9.12	카메라 시스템이 배치되면 무허가 접속을 막기 위해 카메라가 시설 부지와 민감한 영역을 모니터링해야 합니다. 민간한 영역에 대한 무허가 접속을 회사에 알리는 데 경보기가 사용되어야 합니다.	보관 영역은 필요에 따라 화물 처리 및 보관 영역, 중요한 문서가 있는 선적/수령 영역, IT 서버, 국제 교역 도구(IT)를 위한 야적장과 보관 영역, IIT 를 검사하는 영역, 봉인 보관 영역을 포함합니다.	권장

ID	기준	시행 안내	필수/권장
9.13	카메라 시스템이 설치되면 카메라는 수입/수출 과정에 관련된 시설의 주요 영역을 촬영할 수 있는 위치에 베치되어야 합니다. 카메라는 현실적으로 가능한 범위에서 최상의 녹화 품질 세팅에서 녹화를 하도록 프로그램이 되며 매일 24 시간 녹화되도록 세팅이 되어야 합니다.	시설의 통제 아래 있는 물리적 "관리 연속성"을 카메라가 최대한 많이 녹화하기 위해 카메라의 위치를 정확하게 배치하는 것이 중요합니다. 위험 정도에 따라 주요 영역이나 과정에 화물 처리 및 보관, 선적/수령, 화물 적재 과정, 봉인 과정, 수송차 도착/출고, IT 서버, 컨테이너 검사(보안 및 농업), 봉인 보관소 그리고 국제 선적에 관련된 다른 영역이 포함될 수 있습니다.	필수
9.14	카메라 시스템이 설치되는 경우, 카메라에 "작동/녹화 고장"을 표시하는 경보/통보 기능이 있어야 합니다.	비디오 감시 체계의 고장은 누군가가 비디오 상에서 범죄 증거를 남기기 않고 공급망을 침투하려고 시스템을 폐쇄한 결과일 수 있습니다. 기능 작동 고장의 결과로 기기에 즉각적인 주의가 필요하다는 내용을 통지하는 전자 통지문이 미리 지정된 사람에게 보내질 수 있습니다.	권장

ID	기준	시행 안내	필수/권장
	준수되는지 확인하기 위해 카메라 영상을 (경영진, 보안 직원이나 다른 지정 직원이) 정기적으로 무작위 검토를 해야 합니다. 취해진 시정 조치를 포함하는 검토 결과를 요약하여 문서로 보관해야 합니다. 감사를 위해 검토 결과를 충분한 기간 동안 보관해야 합니다.	조사의 일환)가 있을 때만 검토를 하게 되면 카메라 설치가 주는 모든 이점을 사용하지 못하는 것입니다. 카메라는 단지 조사 도구로만 쓰이는 것이 아닙니다. 카메라를 적극적으로 활용하면 보안 침입 발생 자체가 일어나는 것을 막을 수도 있습니다. 영상을 무작위 검토할 때 선적이 안전하고 모든 보안 규정이 지켜지는지 확인하기 위해 물리적 관리 연속성에 집중하십시오. 검토할만한 과정의 예는 다음을 포함합니다. • 화물 처리 활동 • 컨테이너 검사 • 적재 절차 • 봉인 과정 • 수송차 도착/출고 • 화물 출발 등 **검토 목적:** 설치된 보안 과정의 전반적인 준수와 효율성을 평가하고, 인식된 취약점이나 감지된 허점을 찾아내며, 보안 과정 개선을 지원하는 시정 조치를 지시하는 것이 검토를 하는 목적입니다. 위험 정도(이전 사건이나 적재 부두에서 보안 규정을 지키지 않은 직원에 대한 익명의 신고 등)에 따라 회원은 정기적인 검토를 목표로 삼을 수 있습니다.	

ID	기준	시행 안내	필수/ 권장
		요약 문서에 포함되어야 하는 사항: • 검토 날짜 • 영상을 검토한 날짜 • 녹화가 어떤 카메라/영역에서 되었는가 • 발견한 것에 대한 간단한 기술 • 필요한 경우 시정 조치	
9.16	카메라 시스템이 배치되는 경우, 조사가 종료될 수 있도록 주요 수입/수출 과정을 촬영하는 영상 기록을 충분한 기간 보관하고 있어야 합니다.	보안 침입이 발생하면 조사가 이루어지게 되는데, (수출용) 포장과 적재/봉인 과정을 촬영한 카메라 영상을 보관하는 것이 침입 당한 공급망 장소를 알아내는 데 절대적인 도움이 됩니다. 선적이 첫 번째 보급 지점에 도착한 후 적어도 14 일을 모니터링에 할애할 것을 CTPAT 프로그램은 권합니다. 이때가 컨테이너가 관세를 통과한 후 처음으로 개봉되는 때입니다.	권장

10. 물리적 접근 통제 – 접근 통제는 시설/영역의 무허가 접근을 막고 직원과 방문자 통제 관리에 도움을 주며 회사 자산을 보호합니다. 접속 통제에는 모든 진입점에서 모든 직원, 방문자, 서비스 제공자 그리고 하도급 업체에 대해 분명한 신원 확인을 하는 것이 포함됩니다.

ID	기준	시행 안내	필수/권장
10.1	CTPAT 회원은 신원 확인 배지와 접근 기기를 부여하고 변경하며 철회하는 방법을 대해 문서화된 절차를 갖추고 있어야 합니다. 필요한 경우, 확실한 신원 확인과 접근 통제 목적의 직원 신원 확인 시스템이 있어야 합니다. 민감한 영역의 접근은 직무 기술이나 지정된 직무에 기초해 통제되어야 합니다. 직원이 회사를 그만두는 경우 접근 기기는 제거되어야 합니다.	접근 기기에는 직원 신원 확인 배지, 방문자 및 하도급 업체용 임시 배지, 생체 인증 시스템, 비접촉 열쇠 카드, 코드 그리고 열쇠가 포함됩니다. 직원이 회사를 그만두는 경우, 퇴사 점검 목록을 사용하면 모든 접근 기기를 돌려받고/돌려받거나 비활성화했다는 것을 확인하는 데 도움이 됩니다. 직원이 서로를 잘 아는 작은 회사의 경우, 신원 확인 시스템이 필요 없습니다. 일반적으로 50 명이 넘는 직원을 둔 회사에서는 신원 확인 시스템이 필요합니다.	필수

ID	기준	시행 안내	필수/권장
10.2	방문자, 하도급 업체 그리고 서비스 제공자는 사진이 들어간 신분증을 도착 시 제시해야 하고, 상세 방문 내역을 기록한 일지를 보관하고 있어야 합니다. 모든 방문자는 안내를 받아야 합니다. 또한, 모든 방문자와 서비스 제공자에게는 임시 신분 확인증이 발급되어야 합니다. 임시 신분 확인증을 사용하는 경우, 그것을 방문 때마다 잘 보이도록 착용해야 합니다. 등록 일지에는 다음 사항이 포함되어야 합니다. • 방문 날짜 • 방문자 이름 • 사진이 들어간 신분증 (면허증이나 정부 신분증 같이 인증된 유형) 확인. 고정 하도급 업체와 같이 익히 알려진 잦은 방문자의 경우 사진 신분증 검사는 하지 않을 수 있지만 시설에 들어가고 나간 시간은 계속 일지에 기록해야 합니다. • 도착 시간 • 회사 연락 담당 • 떠난 시간		필수

ID	기준	시행 안내	필수/권장
10.3	화물을 배달하거나 수하하는 운전기사는 화물을 수하하거나 출고하기 전에 반드시 확실한 신원 확인이 되어야 합니다. 운전기사는 신원 확인을 받기 위해 정부 발행 사진 신분증을 접근을 허락하는 시설 직원에게 제시해야 합니다. 정부 발행 사진 신분증을 제시하는 것이 현실성이 없는 경우, 시설 직원은 화물을 수거해 가는 운전기사를 채용하는 고속도로 운송 회사가 발행한 사진이 들어간 신분증을 허용된 양식으로 받아들일 수 있습니다.		필수

ID	기준	시행 안내	필수/권장
10.4	운전기사를 등록하고 화물을 수거해 가는 시점의 수송차 상세 내역을 기록하는 화물 수거 일지가 있어야 합니다. 운전기사가 화물 수거를 위해 시설에 도착하면 시설 직원은 운전기사를 화물 수거 일지에 등록해야 합니다. 시설을 떠날 때 운전기사는 나가는 시간을 기록해야 합니다. 화물 일지는 안전하게 보관이 돼야 하며 운전기사에게 접근을 허용해서는 안 됩니다. 화물 수거 일지에는 다음 사항이 기록되어 있어야 합니다. • 운전기사 이름 • 도착 날짜와 시간 • 고용주 • 트럭 번호 • 트레일러 번호 • 시설을 나간 시간 • 나간 시점에 선적에 부착된 봉인 번호	추가 정보를 기록하는 경우, 방문자 일지가 화물 일지로 이중 역할을 할 수 있습니다.	필수

ID	기준	시행 안내	필수/권장
10.7	도착 전 운송 회사는 예정된 수거를 위한 추정 도착 시간, 운전기사의 이름 그리고 트럭 번호를 시설에 통보해야 합니다. 운영상 가능한 경우, CTPAT 회원은 예약을 통한 배달과 수거만을 허용해야 합니다.	이 기준은 송하인과 운송 회사가 가짜 수거를 피하는 데 도움이 됩니다. 가짜 수거는 트럭 운전기사가 가짜 신분증 그리고/또는 화물 절도를 위해 가짜로 차린 사업 등의 속임수를 써서 화물을 훔치는 결과를 가져오는 범죄 계획입니다. 특정 시설에서 상품을 수거하는 고정 운전기사를 둔 운송 회사의 경우 사진과 함께 운전기사 목록을 가지고 있는 것이 좋은 관행입니다. 따라서 현실적으로 회사가 어떤 운전기사가 오는지 알려줄 수 없는 경우에도 회사는 시설에서 화물을 수거하도록 승인을 받았다는 것을 확인할 수 있습니다.	권장
10.8	도착하는 소포나 우편물은 반입 전에 밀수품인지 확인하는 검사를 정기적으로 해야 합니다.	그러한 밀수품에는 폭발물, 불법 마약 그리고 현금을 포함하지만 이에 국한되지는 않습니다.	권장
10.10	보안 요원을 쓰는 경우, 보안 요원에 대한 작업 지침이 문서화된 정책과 절차에 들어 있어야 합니다. 경영진은 이런 절차의 준수와 적정성을 감사와 정책 검토를 통해 정기적으로 확인해야 합니다.	어느 시설이나 보안 요원을 고용할 수 있지만, 흔히 제조 현장, 항구, 보급 센터, 국제 교역 도구 보관 야적장, 혼재업소 그리고 운선 주선업자 영업 현장에서 보안 요원을 고용합니다.	필수

11. 직원 보안 – 회사의 인적 자원은 가장 중요한 자산 중 하나이지만 동시에 가장 취약한 부분일 수도 있습니다. 이 분야의 기준은 직원 심사와 고용 전 확인과 같은 사안에 초점을 두고 있습니다.
많은 보안 침입은 한 명 이상의 직원이 공급망 침투를 할 목적으로 보안 절차를 피할 것을 공모하는 내부 음모로 인해 발생합니다. 따라서 회원은 실사를 통해 민감한 직책을 맡는 직원이 믿을만 하고 신뢰할 수 있다는 사실을 확인해야 합니다. 민감한 직책에는 화물이나 화물 관련 문서에 직접 관련된 업무를 하는 직원 그리고 민감한 영역이나 장비의 접속을 관리하는 일을 하는 직원이 포함됩니다. 그런 직책은 선적, 수하, 우편실 직원, 운전기사, 파견 요원, 보안 요원, 적재 작업, 수송차 추적 그리고/또는 봉인 관리를 하는 모든 사람을 포함하지만 이에 국한되지는 않습니다.

ID	기준	시행 안내	필수/ 권장
11.1	채용 후보자를 확인하고 기존 직원을 정기적으로 점검하는 문서화된 절차가 있어야 합니다. 직업 경력과 추천자와 같은 지원 정보는 법에 의해 가능하고 허용된 범위에서 채용 전에 확인해야 합니다.	일부 국가의 노동 및 개인정보 보호법은 모든 지원 정보를 확인하는 것을 허용하지 않을 수 있다는 사실을 CTPAT 는 알고 있습니다. 그러나 허용되는 경우, 지원 정보를 실사를 통해 확인해야 합니다.	필수

ID	기준	시행 안내	필수/권장
11.2	관련된 법적 제한과 전과 데이터베이스 사용 가능성 유무에 따라 직원 신원 조사가 이루어져야 합니다. 직책의 민감성 정도에 따라 직원 신원 조사 요건이 임시직과 계약직까지 적용이 되어야 합니다. 일단 채용이 되면 이유가 있을 때 그리고/또는 직원 직책의 민감성 정도에 따라 정기적인 재조사가 이루어져야 합니다. 직원 신원 조사에는 시, 주, 지방 그리고 전국 데이터베이스를 이용한 직원의 신분과 전과 조사가 포함되어야 합니다. CTPAT 회원과 그 사업 파트너는 지역 법이 허용하는 범위에서 신원 조사 결과를 채용 결정을 할 때 고려해야 합니다. 신원 조사는 신분과 전과 여부에 국한되지 않습니다. 위험이 더 높은 영역의 경우 더 심층적인 조사가 필요할 수 있습니다.		권장
11.5	CTPAT 회원은 기대하는 행위를 포함하고 용인되는 행위를 정의하는 직원 행동 강령을 가지고 있어야 합니다. 처벌이나 징계 절차가 행동 강령에 포함되어야 합니다. 직원/계약직 근무자는 윤리 강령을 읽었으며 그 내용을 이해했다는 것을 서명을 함으로써 인정해야 하며, 이 인정서가 직원의 파일에 문서 기록으로 들어 있어야 합니다.	윤리 강령은 귀하의 사업을 보호하는 데 도움을 주며, 직원에게 어떤 행동을 기대하는지 알려줍니다. 이 강령의 목적은 회사가 용인할 수 있는 행위 기준을 만들고 유지하는 것입니다. 그것은 회사가 전문적인 이미지를 형성하고 건실한 윤리적 문화를 만드는 데 도움을 줍니다. 작은 회사도 윤리 강령이 필요하지만, 이 경우 정교한 체계를 지니거나 복잡한 정보를 담을 필요는 없습니다.	필수

12. 교육,훈련 및 인식 – CTPAT 의 보안 기준은 다층 보안 체계를 형성하기 위한 것입니다. 만약 한 계층의 보안이 무너지면 다른 계층이 보안 침입을 막거나 회사에 침입을 통보하게 됩니다. 다층 보안 프로그램을 실시하려면 여러 부서와 다양한 직원의 활발한 참여와 지원이 필요합니다. 보안 프로그램을 유지하는 중요한 요소 중의 하나가 교육입니다. 직원에게 어떤 것이 위협이며 회사의 공급망을 보호하는 데 그들의 역할이 어떤 식으로 중요한지를 교육하는 것은 공급망 보안 프로그램의 성공과 지속에 있어 중요한 요소입니다. 또한, 직원이 보안 절차가 왜 있어야 하는지를 이해하게 되면 그것을 준수할 가능성이 더 커집니다. 또한, 왜 보안 절차가 있어야 하는지 직원이 이해하게 되면 그것을 준수할 가능성이 훨씬 커집니다.

ID	기준	시행 안내	필수/ 권장
12.1	회원은 공급망 각 지점에서 테러범이나 밀수업자가 노릴 수 있는 시설, 수송차 그리고 화물의 보안 취약점을 인식하고 그 인식을 높일 수 있는 보안 훈련 및 인식 프로그램을 만들고 유지해야 합니다. 훈련 프로그램은 종합적이고 CTPAT 보안 요건을 모두 다루어야 합니다. 민감한 직책의 직원은 그 직책이 요구하는 직무에 맞춘 특별 훈련을 추가로 받아야 합니다. 보안 프로그램의 주요 요소 중 하나가 훈련입니다. 보안 절차가 왜 있어야 하는지를 이해하는 직원은 그것을 준수할 가능성이 커집니다. 보안 훈련이 필요에 따라 역할과 직책에 기초해 직원에게 정기적으로 제공되어야 하며, 신규 채용 직원은 오리엔테이션/직업 기술 훈련의 일부로서 이 훈련을	훈련 주제에는 접속 통제를 보호하고, 내부 음모를 인식하며, 수상한 활동과 보안 사건을 신고하는 것이 포함될 수 있습니다. 가능하면 특수화된 교육에는 직접 시범이 포함되어야 합니다. 직접 시범을 할 때는 학생이 손수 그 과정을 시범 보일 수 있는 시간을 할당해야 합니다. CTPAT 목적상 민감한 직책에는 수입/수출 화물이나 화물 관련 문서에 직접 관련된 업무를 하는 직원 그리고 민감한 영역이나 장비 접속을 관리하는 일을 하는 직원이 포함됩니다. 그런 직책은 선적, 수하, 우편실 직원, 운전기사, 파견 요원, 보안 요원, 적재 작업, 수송차 추적 그리고/또는 봉인 관리를 하는 모든 사람을 포함하지만 이에 국한되지는 않습니다.	필수

ID	기준	시행 안내	필수/ 권장
	받아야 합니다. 회원은 훈련 일지, 참석 기록서(출석부) 혹은 전자 훈련 증명서를 가지고 있어야 합니다. 훈련 기록에는 훈련 날짜, 참석자 이름 그리고 훈련 주제가 들어 있어야 합니다.		

ID	기준	시행 안내	필수/ 권장
12.2	빈 수송차와 국제 교역 도구(IIT)에 대해 보안 및 농업 검사를 하는 운전기사와 다른 직원은 보안과 농업 목적의 수송차/IIT 검사를 하도록 훈련을 받아야 합니다. 사건 또는 보안 침입 후 혹은 회사 절차에 변경이 있으면 필요에 따라 정기적으로 재훈련이 실시되어야 합니다. 검사 훈련에는 다음과 같은 주제가 포함되어야 합니다. • 숨겨진 칸이 있다는 표시 • 자연적으로 생기는 칸에 숨겨진 밀수품 • 해충 오염의 흔적		필수
12.4	CTPAT 회원은 제공된 훈련이 모든 훈련 목적을 만족시키는지 확인하는 방법을 갖추고 있어야 합니다.	(민감한 업무를 담당하는 직원이) 훈련을 이해하고 그 훈련을 자신의 직책에 적용할 수 있는 것은 매우 중요합니다. 훈련의 효과를 알아보기 위해 실시할 수 있는 방법의 예로 시험이나 퀴즈, 모의 연습/훈련 혹은 절차에 대한 정기 감사 등을 들 수 있습니다.	권장
12.8	필요한 경우, 역할 그리고/또는 직책에 따라 직원은 회사의 사이버 보안 정책과 절차에 대해 훈련을 받아야 합니다. 직원이 암호/암호구 그리고 컴퓨터 접속을 보호하는 것이 이 훈련에 포함됩니다.	품질 관리 훈련은 사이버 공격의 취약점을 줄이는 데 있어 중요합니다. 강력한 사이버 보안 훈련 프로그램은 주로 이메일이나 메모를 통해 단순히 전달되는 것이 아니라 공식적인 환경에서 관련 직원에게 전달되는 프로그램입니다.	필수

ID	기준	시행 안내	필수/권장
12.9	보안 기술 시스템을 운영하고 관리하는 직원은 자신의 특정 영역에 대해 운영 및 관리 훈련을 받아야 합니다. 비슷한 시스템을 이전에 경험한 경우 인정이 됩니다. 조작 설명서나 다른 방법을 통해 독학한 경우도 인정이 됩니다.		필수
12.10	직원은 보안 사건과 수상한 활동을 신고하는 방법에 대해 훈련을 받아야 합니다.	보안 사고와 수상한 활동을 신고하는 절차는 보안 프로그램의 매우 중요한 측면입니다. 사건을 신고하는 방법에 대한 훈련은 전반적인 보안 훈련에 포함되어야 합니다. (직무에 기초한) 특수화된 훈련 모듈은 무엇을 신고하고 사건을 누구에게 어떻게 신고해야 하며 신고를 한 뒤 어떻게 해야 되는지와 같은 과정상 구체적인 사항이 포함된 신고 절차에 대해 더 상세한 훈련을 포함할 수 있습니다.	필수