PCI 데이터 보안 표준

요구사항 및 보안평가 절차

버전 1.2

2008 년 10 월

목차

서론 및 **PCI** 데이터 보안 표준 개요

PCI 데이터 보안 표준(PCI DSS)은 카드회원 데이터 보안을 강화 및 촉진하고, 전 세계적으로 일관된 데이터 보안 평가에 대한 광범위한 채택을 촉진하기 위해 개발되었다. 본 문서(*PCI 데이터 보안 표준 요구사항 및 보안 평가 절차*)는 12 개의 PCI DSS 요구사항들에 기초하며, 상응하는 시험 절차들과 결합하여 보안 평가 도구로 사용한다. PCI DSS 규정 준수 여부를 검증해야 하는 가맹점 및 서비스 제공자들을 대상으로 보안감사를 수행하는 평가자가 사용하도록 본 문서가 설계되었다. 아래는 12 개의 PCI DSS 요구사항들에 대한 상위-수준의 개요이다. 이어지는 페이지들은 PCI DSS 평가의 준비, 수행 및 보고에 대한 배경을 제공하며, 13 페이지에서부터는 상세한 PCI DSS 요구사항들이 이어진다.

PCI 데이터 보안 표준 – 상위-수준 개요

안전한 네트워크를 구축하고 유지한다

요구사항 1: 카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다
요구사항 2: 시스템 패스워드 및 기타 보안 파라미터에 벤더가 제공한 디폴트 값을 사용하지 않는다

카드회원 데이터를 보호한다

요구사항 3: 저장된 카드회원 데이터를 보호한다
요구사항 4: 공중망을 통한 카드회원 데이터 전송을 암호화한다

취약점 관리 프로그램을 유지한다

요구사항 5: 안티바이러스 소프트웨어를 사용하고 정기적으로 갱신한다
요구사항 6: 안전한 시스템과 어플리케이션을 개발하고 유지한다

강력한 접근 통제 대책을 적용한다

요구사항 7: 업무상 알 필요가 있는지에 따라 카드회원 데이터에 대한 접근을 제한한다
요구사항 8: 컴퓨터에 접근하는 사용자별로 고유 ID 를 부여한다
요구사항 9: 카드회원 데이터에 대한 물리적 접근을 제한한다

네트워크를 정기적으로 감시하고 시험한다

요구사항 10: 네트워크 자원과 카드회원 데이터에 대한 모든 접근을 추적하고 감시한다
요구사항 11: 보안시스템 및 프로세스를 정기적으로 시험한다

정보보호 정책을 유지한다

요구사항 12: 정보보호를 위한 정책을 유지한다

PCI DSS 적용범위 정보

다음 표는 카드회원 데이터 및 민감한 인증 데이터에서 공통적으로 사용되는 항목에 대해, 각 데이터 요소의 저장이 허용 혹은 금지되는지, 그리고 각 데이터 정보가 보호되어야 하는지의 여부를 나타낸다. 표에서 빠짐없이 나타난 것은 아니지만, 각 데이터 항목들에 적용하는 다양한 종류의 요구사항들을 보여준다.

	데이터 항목	저장 허용	보호 필요	PCI DSS 요구사항 3.4
카드회원 데이터	Primary Account Number (PAN)	Yes	Yes	Yes
	카드회원 이름 [1]	Yes	Yes [1]	No
	서비스 코드 [1]	Yes	Yes [1]	No
	유효 기간 [1]	Yes	Yes [1]	No
민감한 인증 데이터 [2]	전체 마그네틱 선 데이터 [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

1 *해당 데이터 항목들은 PAN과 함께 저장될 때는 반드시 보호되어야 한다. 이러한 보호는, 카드소유자 데이터 환경의 전반적인 보호에 관련된 PCI DSS 요구사항에 따르게 된다. 추가로, 사업 상 소비자 관련 개인 데이터가 수집되고 있다면, 다른 법률(예를 들어, 소비자 개인 데이터 보호, 사생활, 신원 절도, 데이터 보안과 관련된)이 해당 데이터에 대한 특정한 보호나, 회사 방침의 공개를 요구할 수 있다. 하지만, PAN이 보관, 처리, 혹은 전송되지 않는다면 PCI DSS는 적용되지 않는다.*

2 *민감한 인증 데이터는 암호화 되었다고 하더라도, 승인 이후 절대 보관되어서는 안 된다.*

3 *마그네틱 선이나, 칩 상의 마그네틱 선 이미지 혹은 다른 곳의 전체 트랙 데이터*

PCI DSS 요구사항의 준수를 위한 평가 범위

PCI DSS 보안 요구사항은 모든 시스템 구성 요소에 적용된다. "시스템 구성 요소"는 카드회원 데이터 환경에 포함되거나 연결되어 있는 특정 네트워크 구성 요소, 서버, 혹은 응용 프로그램으로 정의된다. 카드회원 데이터 환경은 카드회원 데이터나 민감한 인증 데이터를 소유한 네트워크의 일부이다. 네트워크 구성 요소가 포함하는 것에는 방화벽, 스위치, 라우터, 무선 AP, 네트워크 장비 및 기타 보안 장비에만 제한되지 않는다. 서버 종류가 포함하는 것에는 웹, 응용 프로그램, 데이터베이스, 인증, 메일, 프록시, 네트워크 타임 프로토콜(NTP) 및 도메인 네임 서버(DNS)에만 제한되지 않는다. 응용 프로그램은 내부 및 외부(인터넷) 응용 프로그램을 포함하여 구매되거나 제작된 모든 응용 프로그램을 포함한다.

네트워크 분리

기업 네트워크의 나머지로부터 카드회원 데이터 환경의 네트워크 분리나 격리(분리)는 PCI DSS 요구사항이 아니다. 하지만, 다음을 감소시킬 수 있는 방법의 하나로 권고된다:

- PCI DSS 평가 범위
- PCI DSS 평가 비용
- PCI DSS 통제의 구현 및 유지를 위한 비용 및 어려움
- 조직에 대한 위험 (카드회원 데이터를 적은 수의 통제된 장소로 통합함에 따른 감소)

적절히 네트워크 분리가 되지 않게 되면 (간혹 "평평한 네트워크"로 불리는) 전체 네트워크가 PCI DSS 평가 범위에 포함된다. 네트워크 분리는 내부 네트워크 방화벽, 강력한 접근통제 목록을 가진 라우터, 혹은 네트워크의 특정 부분으로의 접근을 제한하는 그 밖의 기술로 가능할 수 있다.

카드회원 데이터 환경의 범위를 줄이기 위해서 중요한 필요 조건은 사업적 요구 및 카드회원 데이터의 보관, 처리, 혹은 전송과 연관된 프로세스에 대한 명확한 이해다. 불필요한 데이터의 제거 및 필수 데이터의 통합을 통해서 가능한 한 적은 위치로 카드회원 데이터를 제한하기 위해서는 관례적으로 수행해 오던 업무 프로세스 리엔지니어링을 필요로 할 수도 있다.

데이터흐름 다이어그램에 카드회원 데이터 흐름을 문서화 하게 되면 모든 카드회원 데이터 흐름을 온전히 이해하게 하고 특정 네트워크 분리를 통해 카드회원 데이터 환경을 격리할 때 효과를 갖도록 한다.

만약 네트워크 분리가 적절히 이루어져 PCI DSS 평가 범위를 축소했다면, 평가자는 네트워크 분리가 평가 범위를 축소하는데 알맞은지를 반드시 검증해야 한다. 전반적으로 적절한 네트워크 분리는 카드회원 데이터를 보관, 처리, 혹은 전송하는 시스템을 그렇지 않은 시스템으로부터 격리한다. 하지만, 네트워크 분리의 특정한 구현에 대한 타당성은 변동이 심하고, 주어진 네트워크 설정, 배치된 기술들 및 구현되어 있을 다른 통제들과 같은 것들에 대한 의존이 심하다.

*부록 F: PCI DSS 검토 – 범위 정의 및 표본의 선택*은 PCI DSS 평가에서 범위 선택의 효과와 관련하여 추가 정보를 제공한다.

무선

만약 무선 기술이 카드회원 데이터의 저장, 처리, 혹은 전송에 사용되었거나(예를 들어, POS 거래, “line-busting”), 무선 LAN 이 카드회원 데이터 환경이나 그 일부에 접속되었다면(예를 들어, 방화벽으로 완벽히 분리되지 않은), 무선 환경을 위한 PCI DSS 요구사항과 절차 시험이 적용되며, 이행도 이루어져야 한다(예를 들어, 요구사항 1.2.3, 3.1.1, 그리고 4.1.1). 무선 기술이 구현되기 전에, 회사는 위험에 비추어 기술의 필요성을 신중히 평가해야 한다. 민감하지 않은 데이터 전송을 위해서만 무선 기술이 배치되도록 고려한다.

제 3 자/아웃소싱

매년 보안감사를 받아야 하는 서비스 제공자의 경우, 카드회원 데이터가 보관, 처리, 혹은 전송되는 모든 시스템 구성 요소를 대상으로 준수 여부에 대한 검증이 이루어져야 한다.

서비스 제공자나 가맹점은 그들을 대신해서 카드회원 데이터의 보관, 처리, 전송 업무에, 또는 라우터, 방화벽, 데이터베이스, 물리적 보안, 서버와 같은 구성 요소들을 관리하기 위해 제 3 의 제공자를 사용할 수 있다. 만약 그렇다면, 카드회원 데이터 환경의 보안에 영향이 있을 것이다.

제 3 의 서비스 제공자에게 카드회원 데이터의 저장, 처리, 전송을 아웃소싱 하는 사업체들의 경우에는, 준수보고서(ROC)에 어떤 요구사항이 검토 사업체에 적용되고 어떤 요구사항이 서비스 제공자에게 적용되는지를 명확히 구분하여 각 서비스 제공자의 역할을 문서화해야 한다. 제 3 의 서비스 제공자들을 대상으로 준수 여부를 검증하는 두 가지 방법이 있다: 1) 서비스 제공자가 PCI DSS 평가를 받고 고객들에게 준수 여부를 입증하거나, 2) 서비스 제공자가 PCI DSS 평가를 받지 않았다면, 고객들의 PCI DSS 평가 각 과정 동안 서비스 제공자의 서비스에 대해서 평가를 받아야 한다. “준수보고서를 위한 지침 및 항목” Part 3 밑에 점으로 시작하는 “관리 서비스 제공자(MSP) 검토” 에서 보다 많은 정보를 확인할 수 있다.

추가로, 가맹점과 서비스 제공자는 카드회원 데이터에 접근하는 모든 관련된 제 3 자의 PCI DSS 준수 여부를 반드시 관리하고 모니터링해야 한다. *자세한 내용은 이 문서의 요구사항 12.8 에서 참고하라.*

업무 시설 및 시스템 구성 요소의 표본 추출

평가자는 PCI DSS 요구사항을 평가하기 위해 업무 시설 및 시스템 구성 요소를 대표하는 표본을 선택할 수 있다. 표본은 반드시 업무 시설 및 시스템 구성 요소를 포함해야 하며, 시스템 구성 요소의 종류는 물론 업무 시설의 종류 및 위치 모두를 대표하는 선택이 되어야 하고, 통제가 기대하는 수준으로 구현되어 있다는 것에 대해 평가자가 보증하기에 충분한 크기여야 한다.

업무 시설의 예로는 회사 사무실, 상점, 체인점 및 여러 곳에 위치해 있는 업무 시설들을 들 수 있다. 표본 추출은 각 업무 시설 별 시스템 구성 요소를 포함해야 한다. 예를 들어, 각 업무 시설 별로, 여러 종류의 운영 체제, 기능 및 검토 대상 영역에 적용 가능한 응용 프로그램을 포함한다. 각 업무 시설 내에서, 검토자는 Apache WWW 를 구동하는 Sun 서버, Oracle 을 구동하는 Windows 서버, 오래된 카드 처리 응용 프로그램을 구동하는 메인프레임 시스템, HP-UX 를 구동하는 데이터 전송 서버, MYSQL 을 구동하는 Linux 서버를 고를 수 있다. 만약 모든 프로그램이 단일의 OS(예를 들어, Windows 혹은 Sun)에서 동작한다고 해도, 표본은 여러 가지의 응용 프로그램(예를 들어, 데이터베이스 서버, 웹 서버, 데이터 전송 서버)을 포함해야 한다. (*부록 F: PCI DSS 검토 – 범위 정의 및 표본의 선택을 참고하라.*)

업무 시설 및 시스템 구성 요소의 표본 선택 시, 평가자는 다음 사항을 고려해야 한다:

- 각 시설이 표준 프로세스에 따라 구성되었음을 확인하기 위한 표본의 규모는, 각 시설이 반드시 준수해야 하는 표준화된 PCI DSS 프로세스가 수립되어 있을 때는, 표준화된 프로세스가 없을 때보다는, 작아질 수 있다.
- 만약 한 종류 이상의 표준 프로세스가 존재한다면(예를 들어, 시스템 구성요소나 시설에 대한 각각의 종류), 표본은 반드시 각각의 프로세스에 의해 보안이 준수되어야 하는 시스템 구성요소나 시설을 포함할 수 있도록 충분히 커야 한다.
- 표준 PCI DSS 프로세스가 없고 각 시설이 각자의 프로세스를 가지고 있다면, 표본 크기는 반드시 각 시설이 PCI DSS 요구사항을 적절히 이해하고 구현하고 있음을 보증할 정도로 커야 한다.

부록 F: PCI DSS 검토 – 범위 정의 및 표본의 선택을 함께 참조하라.

보완 통제

부록 B: 보완 통제 및 *부록 C: 보완 통제 워크시트*에 따라 매년 모든 보완 통제는 반드시 문서화 및 검토되고 평가자에 의해 검증되어, 표준 준수 보고서 제출 시에 포함되어야 한다.

각각의 모든 보완 통제 별로 보완 통제 워크시트(부록 C)가 **반드시** 작성되어야 한다. 추가적으로, 보완 통제 결과는 표준 준수 보고서의 해당 PCI DSS 요구사항 부분에 문서화되어야 한다.

"보완 통제"에 대해 보다 자세한 내용은 위에서 언급된 부록 B 와 C 를 참조하라.

표준 준수 보고서를 위한 지침 및 내용

이 문서는 반드시 *표준 준수 보고서* 작성을 위한 템플릿으로 사용되어야 한다. 평가를 완료한 사업체는 각 지급결제 브랜드가 사업체의 준수 상태를 확인할 수 있도록 각 지급결제 브랜드의 해당 보고 요구사항을 따라야 한다. 보고 요구사항 및 지침을 확인하기 위해서는 각 지급결제 브랜드에 연락하라.

보고서 내용 및 형식

표준 준수 보고서를 작성할 때 보고서 내용 및 형식은 다음 지침을 따르라.

1. 개요

포함 내용:

- 다음을 포함하여 사업체의 지급결제 카드 사업을 기술한다:
  - 카드회원 데이터의 보관, 처리, 전송의 방법과 이유 등 지급결제 카드와 관련된 사업체의 역할
    참고: 사업체의 웹 사이트에서 복사하여 붙여 넣으려 하지 말고, 평가자가 지급결제 및 사업체의 역할을 이해한 내용을 반영하여 작성해야 함.
  - 사업체의 지급결제 처리 방법 (직접, 간접, 기타)
  - 제공하는 지급결제 경로의 유형. 비대면 (예를 들어, 통신 판매(MOTO), 전자상거래) 또는 대면
  - 프로세서 관계를 포함하여, 지급결제 전송이나 처리에 연결하는 모든 사업체
- 다음 사항을 포함하여 사업체의 네트워크 현황에 대한 개략적인 네트워크 다이어그램(사업체로부터 획득하거나 평가자가 작성)
  - 네트워크 내·외부로의 연결
  - 카드회원 데이터 환경 내의 주요 구성요소 (해당하는 POS 장비, 시스템, 데이터베이스, 그리고 웹 서버를 포함)
  - 해당하는 기타 필요한 지급결제 구성요소

2. 작업 범위 및 수행 방법의 기술

이 문서의 '평가 범위' 부분에 따라, 다음과 같이 범위를 기술

- 중점 평가 대상 환경 (예를 들어, 고객의 인터넷 AP, 내부 기업 네트워크, 처리 연결들)
- 만약 네트워크 분리가 적절히 이루어지고 PCI DSS 검토의 범위를 줄이기 위해 사용되었다면, 분리 현황과 분리가 효과적인지를 평가자가 어떻게 검증하였는지를 간략히 기술
- 선정된 사업체(상점, 업무시설 등)와 시스템 구성요소 모두에 대해 사용한 표본 추출의 문서화 및 사유 기술
  - 전체 모집단
  - 표본의 수
  - 선택된 표본의 근거
  - 검토한 통제항목들이 사업체에 적용된 통제항목들을 대표한다고 평가자가 판단할 수 있도록 표본 규모가 충분한 이유
  - 검토의 범위로부터 '제외된' 카드회원 데이터의 보관, 처리, 전송되는 모든 위치나 환경, 그리고 왜 해당 위치/환경이 제외되었는지 사유를 기술
- PCI DSS 를 준수해야 하는 100% 지분을 보유한 모든 자회사들을 나열하고, 자회사들이 개별적으로 검토되거나 본 평가의 일부분으로써 검토되었는지의 여부 기술
- PCI DSS 를 준수해야 하는 모든 해외 사업체들을 나열하고, 사업체들이 개별적으로 검토되거나 본 평가의 일부분으로써 검토되었는지의 여부 기술
- 카드회원 데이터에 연결되거나 보안에 영향을 줄 수 있는 모든 무선 LAN, 무선 지급결제 어플리케이션(예를 들어, POS 단말기)을 나열하고, 해당 무선 환경에 적용된 보안의 기술
- 평가를 수행하는데 사용된 'PCI DSS 요구사항 및 보안 평가 절차' 문서의 버전
- 평가 기간

3. 검토된 환경의 세부 사항

이 부분에서는 다음 세부 사항을 포함한다:

- LAN, WAN, 인터넷을 포함하는 통신 연결의 각 부분에 대한 다이어그램
- 카드회원 데이터 환경에 대한 기술, 예를 들어:
  - 해당하는 승인, capture, 정산, 지불 거절(chargeback) 및 기타 흐름을 포함하는 카드회원 데이터의 전송 및 처리에 대한 문서화
  - 카드회원 데이터를 저장하고 있는 파일과 테이블의 목록. 평가자는 목록을 작성(또는 고객으로부터 입수)하여 작업 문서(work paper)에 첨부하여 보존해야 한다. 각각의 카드회원 데이터 저장소 별로(파일, 테이블 등) 목록은 다음을 포함해야 한다:
    - 저장된 카드회원 데이터의 모든 요소에 대한 목록

  - 데이터 보호 방법
  - 데이터 저장소 접근에 대한 로그 기록 방법
- 카드회원 데이터 환경에 사용되고 있는 하드웨어와 중요 소프트웨어의 목록, 각각의 기능/용도에 대한 기술
- 회사가 카드회원 데이터를 공유하는 서비스 제공자 및 기타 사업체의 목록 (주: 해당 사업장들은 PCI DSS 요구사항 12.8 에 적용됨)
- 사용중인 제 3 자 지급결제 어플리케이션 제품 및 버전의 목록. 각 지급결제 어플리케이션이 PA-DSS 에 따라 검증되었는지 여부 포함. 지급결제 어플리케이션이 PA-DSS 검증을 받았을지라도, 평가자는 해당 어플리케이션이 PCI DSS 를 준수하는 방법과 환경으로 구현되고, 지급결제 어플리케이션 벤더의 PA-DSS '*구현 가이드*'에 따라서 구현되어 있는지 확인할 필요가 있다. *주: PA-DSS 에 따라 검증된 어플리케이션의 사용이 PCI DSS 요구사항은 아니다. PA-DSS 준수 요구사항을 이해하기 위해서는 각 지급결제 브랜드와 개별적으로 상의하라.*
- 인터뷰 대상자와 그들의 직함 목록
- 검토한 문서의 목록
- 관리 서비스 제공자(MSP)의 검토에 있어, 평가자는 MSP 에 적용하는(그리고 검토에 포함되는) 이 문서의 요구사항들과, 검토에 포함하지 않고 MSP 의 고객이 검토에 포함시킬 책임이 있는 요구사항들을 명확하게 식별해야 한다. MSP 의 분기별 취약점 스캔의 일부로서 스캔하는 IP 주소, 그리고 MSP 의 고객이 분기별 취약점 스캔에 포함하여야 하는 IP 주소에 대한 정보를 포함해야 한다.

4. 연락처 정보 및 보고 날짜

다음을 포함:

- 가맹점, 서비스 제공자, 평가자에 대한 연락처 정보
- 보고 날짜

5. 분기별 스캔 결과

- 'Executive Summary'와 요구사항 11.2 의 설명란에 최근 4 분기의 스캔 결과를 요약

  참고: 평가자가 다음 사항들을 확인하였다면 최초의 PCI DSS 준수에 분기별로 통과된 취약점 스캔이 4 번 필요한 것은 아니다. 1) 가장 최근의 스캔 결과가 통과되었고, 2) 사업체가 분기별 스캐닝을 요구하는 정책 및 절차를 문서화 했고, 3) 최초 스캔에 기록된 모든 취약점들이 다시 스캔한 결과 조치되었음. 최초의 PCI DSS 검토 이후, 다음 연도는 분기별로 4 번의 스캔이 반드시 이루어져야 한다.
- 스캔은 '*PCI DSS 보안 스캐닝 절차*'에 따라서 사업체에 존재하는 모든 외부에서 접근 가능한(인터넷과 접하는) IP 주소를 포함해야 한다.

6. 결과 및 의견

- 표준 준수 보고서 템플릿 형식에 맞춰지지 않을 수 있는 모든 결과를 'Executive Summary'에 요약하라.
- 모든 평가자들은 각 요구사항 및 하위-요구사항의 자세한 보고서 서술 및 결과를 제공하기 위해 *반드시* '상세 PCI DSS 요구사항 및 보안 평가 절차' 템플릿을 사용해야 한다.
- 평가자는 통제가 적절히 적용되었다는 결론을 내기 위하여 고려한 모든 보완 통제를 *반드시* 검토하고 문서화해야 한다.

  비고: "보완 통제"에 대해 보다 자세한 설명은 앞의 '보완 통제' 부분과 부록 B 와 C 를 참고하라.

미결 항목의 재 검증

준수를 확인하기 위해 "적용한 통제항목" 보고서가 필요하다. "미결 항목"을 포함하거나, 미래에 완료될 항목을 포함한다면, 보고서는 비-준수한 것으로 간주된다. 가맹점/서비스 제공자는 검증이 완료되기 전에 반드시 해당 항목들을 처리해야 한다. 가맹점/서비스 제공자에 의해 해당 항목들이 처리된 이후에, 평가자는 조치가 이루어지고 모든 요구사항이 만족되는지를 검증하는 재평가를 하게 된다. 재검증 이후에, 평가자는 카드회원 데이터 환경이 충분히 준수됨을 검증하고, (아래) 지침에 따라 보고서를 제출하게 된다.

PCI DSS 준수 – 완료 절차

1. "표준 준수 보고서를 위한 지침 및 항목"이라고 이름 붙은 상단 부분을 따라서 '표준 준수 보고서' (ROC)를 완성하라.
2. 통과된 취약점 스캔이 'PCI SSC 인증 스캐닝 벤더' (ASV)에 의해 수행되었는지 확인하고, ASV 로부터 통과된 스캔의 증거를 입수하라.
3. 해당되는 '서비스 제공자'나 '가맹점'용 '준수 증명서'를 양식대로 작성하라. '준수 증명서'는 부록 D 와 E 를 참조하라.
4. ROC, 통과된 스캔의 증거, 그리고 '준수 증명서' 및 제반 문서를 (가맹점의 경우) 매입사에, (서비스 제공자의 경우) 지급결제 브랜드나 기타 요청자에게 제출하라.

상세 **PCI DSS** 요구사항 및 보안 평가 절차

*'PCI DSS 요구사항 및 보안 평가 절차'*에서 사용되는 표에서의 열 제목을 다음과 같이 정의한다:

- **PCI DSS 요구사항** – 이 열은 '데이터 보안 표준'을 정의하고 PCI DSS 준수를 달성하기 위한 요구사항들을 나열한다; 준수는 이 요구사항들에 대하여 검증될 것이다.
- **시험 절차** – 이 열은 PCI DSS 요구사항이 "적용"되었다는 것을 검증하기 위해 평가자가 수행해야 하는 프로세스들을 보여준다.
- **적용** – 이 열은, 보완 통제의 결과로 적용된 통제들을 포함하여, 적용된 통제들에 대한 간결한 서술을 제공하기 위해서 반드시 평가자에 의해 사용되어야 한다. (참고: 이 열은 아직 적절하지 않은 항목이나 미래에 완료될 공개 항목을 위해 사용되어서는 절대로 *안 된다*.)
- **미적용** – 이 열은 미적용 통제에 대한 간결한 서술을 제공하기 위해서 반드시 평가자에 의해 사용되어야 한다. 미준수 보고서는 별도로 요청되지 않는 한은 지급결제 브랜드나 매입사에 제출되어서는 안 된다. 미준수 보고서에 대한 보다 많은 지침은 부록 D 와 부록 E: 준수 증명서를 참조하라.
- **목표일/설명** – "미적용" 통제들에 대해 평가자는 가맹점이나 서비스 제공자들이 통제를 "적용" 하기를 기대하는 목표일을 기재할 수 있다. 모든 추가적인 기록이나 설명은 마찬가지로 여기에 포함될 수 있다.

안전한 네트워크를 구축하고 유지한다

요구사항 1: 카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다.

방화벽은 회사 네트워크(내부)와 신뢰되지 않은 네트워크(외부)의 허용된 컴퓨터 트래픽 뿐만 아니라 회사 내부 네트워크 상에서 보다 중요한 영역을 통과하는 트래픽을 통제하는 장비이다. 카드회원 데이터 환경은 회사의 위탁된 네트워크에 좀더 중요한 영역의 예시가 된다.

방화벽은 모든 네트워크 트래픽을 검사하여 명시된 보안기준에 맞지 않은 트래픽을 차단한다.

전자상거래를 위한 시스템, 임직원의 데스크탑 브라우저를 통한 인터넷 접속, 이메일 접속, 특정 목적을 가진 B2B 연결, 무선 네트워크 또는 다른 곳을 경유한 소스들 등 모든 시스템은 신뢰되지 않은 네트워크의 비 인가된 접근으로부터 보호되어야 한다. 인터넷에 연결된 경로 중 표면적으로는 중요성이 떨어진 경로를 통해 중요한 시스템으로 불법 접근할 수 있는 취약점이 있는 경우도 있다. 방화벽은 컴퓨터 네트워크를 보호하기 위한 핵심 메커니즘이라 할 수 있다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
1.1 아래 사항을 포함하여 방화벽과 라우터 설정 기준을 만들어야 한다:	1.1 기준이 완전한지 확인하기 위해 아래에 명시된 방화벽과 라우터 설정 기준 및 관련 문서를 확보하고 검사한다. 아래 사항을 수행한다:			
1.1.1 모든 네트워크 접속 및 방화벽과 라우터 설정 변경사항을 승인하고 테스트하는 공식 절차	1.1.1 모든 네트워크 접속 및 방화벽과 라우터 설정 변경사항을 테스트하고 승인하는 공식 절차가 있는지 확인한다.			
1.1.2 무선 네트워크를 포함하여 카드회원 데이터에 대한 모든 접속을 표시한 최신 네트워크 구성도	1.1.2.a 현재의 네트워크 구성도가 있는지 확인하고 (예: 네트워크 상에서 카드회원 데이터 흐름이 포함된 네트워크 구성도), 이 네트워크 구성도가 무선 네트워크를 포함하여 카드회원 데이터로의 모든 연결을 보여 주고 있는지 확인한다.			
	1.1.2.b 네트워크 구성도가 최신 상태로 되어 있는지 확인한다.			
1.1.3 모든 인터넷 접속 지점, DMZ 와 내부 네트워크 구역 사이의 방화벽 설치에 대한 요구사항	1.1.3 방화벽 설정 기준이 모든 인터넷 접속 지점, DMZ 와 내부 네트워크 구역 사이의 방화벽 설치에 대한 요구사항을 포함하고 있는지 확인한다. 현재의 네트워크 구성도가 방화벽 설정 기준과 일치하는지 확인한다.			
1.1.4 네트워크 구성요소의 논리적 관리를 위한 조직, 역할 및 책임에 대한 정의	1.1.4 방화벽과 라우터 설정 기준에 네트워크 구성요소의 논리적 관리를 위한 조직, 역할 및 책임에 대한 정의가 포함되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
1.1.5 모든 서비스, 프로토콜, 포트의 사용에 대한 문서화 및 사용 근거를 명시하고, 안전하지 못한 프로토콜에 대해서는 적용한 보안 기능에 대한 문서화	1.1.5.a 방화벽과 라우터 설정 기준에 업무에 필요한 서비스, 프로토콜, 포트 목록이 문서화되어 있는지 확인한다. 예: HTTP (hypertext transfer protocol), SSL (Secure Sockets Layer), SSH (Secure Shell), VPN (Virtual Private Network) 프로토콜.			
	1.1.5.b 허용된 안전하지 못한 서비스, 프로토콜, 포트를 확인한다. 각 서비스에 대한 방화벽과 라우터의 설정 기준 및 설정값을 검사하여 서비스의 필요 여부와 보안 기능이 문서화되고 적용되어 있는지 확인한다. 안전하지 못한 서비스, 프로토콜, 포트의 예로는 사용자 증명이 평문으로 통과하는 FTP 가 있음			
1.1.6 최소 6 개월 마다 방화벽과 라우터 룰셋에 대한 검토 요구사항	1.1.6.a 방화벽과 라우터의 설정 기준에 방화벽과 라우터의 룰 셋을 최소 6 개월 마다 점검하도록 요구하고 있는지를 확인한다.			
	1.1.6.b 룰셋이 최소 6 개월 마다 검토되고 있는지 확인하기 위해 문서를 받아 확인한다.			
1.2 신뢰할 수 없는 네트워크와 카드회원 데이터 환경의 모든 시스템 구성요소 사이에 접속을 제한하는 방화벽 설정을 적용한다.	1.2 신뢰할 수 없는 네트워크와 카드회원 데이터 환경의 시스템 구성요소 사이에 접속을 제한하고 있는지 확인하기 위하여 방화벽과 라우터 설정을 다음과 같이 점검한다:			
참고: "신뢰할 수 없는 네트워크"는 검토 대상 사업체에 속한 네트워크와 관계없는, 그리고/혹은 통제나 관리에 있어 사업체의 능력을 벗어나는 모든 네트워크이다.				
1.2.1 카드회원 데이터 환경에 필요한 트래픽으로 인바운드 및 아웃바운드 트래픽을 제한한다.	1.2.1.a 카드회원 데이터 환경에 필요한 트래픽으로 인바운드 및 아웃바운드 트래픽이 제안되어 있고, 제한내역이 문서화 되어있는지 확인한다.			
	1.2.1.b 모든 기타 인바운드 및 아웃바운드 트래픽이 구체적으로 거부되고 있는지 점검한다. 예를 들면, 명백한 "deny all" 혹은 allow 문 뒤에 암묵적인 deny 를 사용함.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
1.2.2 라우터 설정 파일의 보호 및 동기화	1.2.2 라우터 설정 파일이 보호되고 동기화 되어 있는지 점검한다. 예를 들면, running 설정 파일 (라우터의 일반적인 구동에 필요)과 start-up 설정 파일 (재부팅 될 때 사용)이 동일하면서 안전한 설정임.			
1.2.3 모든 무선 네트워크와 카드회원 데이터 환경 사이에 경계 방화벽을 설치하고, 이 방화벽을 설정하여 무선 환경으로부터 카드회원 데이터 환경으로 오는 모든 트래픽을 거부 혹은 제어(업무 목적상 필요한 트래픽인 경우)한다.	1.2.3 모든 무선 네트워크와 카드회원 데이터를 보관하는 시스템 사이에 경계 방화벽이 설치되어 있고, 이 방화벽이 무선 환경으로부터 카드회원 데이터 환경으로 오는 모든 트래픽을 거부 혹은 제어(업무 목적상 필요한 트래픽인 경우)하는지 확인한다.			
1.3 인터넷과 카드회원 데이터 환경의 모든 시스템 구성요소 사이에 외부자의 직접 접근을 제한한다.	1.3 방화벽과 라우터의 설정을 아래 명시한 바대로 조사하여 인터넷과 시스템 구성요소(인터넷의 내부 라우터, DMZ 라우터와 방화벽, DMZ 카드회원 세그먼트, 경계 라우터, 그리고 내부 카드회원 네트워크 세그먼트를 포함) 사이에 직접 접근이 없는지 확인한다.			
1.3.1 카드회원 데이터 환경에 필요한 프로토콜만 가능하도록 인바운드 및 아웃바운드 트래픽을 제한하는 DMZ 를 구현한다.	1.3.1 카드회원 데이터 환경에 필요한 프로토콜만 가능하도록 인바운드 및 아웃바운드 트래픽을 제한하는 DMZ 를 구현하였는지 확인한다.			
1.3.2 인바운드 인터넷 트래픽을 DMZ 내의 IP Address 로 제한한다.	1.3.2 인바운드 인터넷 트래픽을 DMZ 내의 IP Address 로 제한하고 있는지 확인한다.			
1.3.3 인터넷과 카드회원 데이터 환경 사이의 트래픽에 대해서 인바운드 혹은 아웃바운드의 직접 경로를 허용하지 않는다.	1.3.3 인터넷과 카드회원 데이터 환경 사이의 트래픽에 대해서 인바운드 혹은 아웃바운드의 직접 경로를 허용하지 않는지 확인한다.			
1.3.4 내부 주소가 인터넷에서 DMZ 로 전달되도록 허용하지 않는다.	1.3.4 내부 주소가 인터넷에서 DMZ 로 전달되지 않는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
1.3.5 카드회원 데이터 환경에서 인터넷으로의 아웃바운드 트래픽을 제한하여 아웃바운드 트래픽이 DMZ 내의 IP 주소만 접근하게 한다.	1.3.5 카드회원 데이터 환경으로부터 인터넷으로의 아웃바운드 트래픽이 DMZ 내의 IP 주소만 접근할 수 있는지 확인한다.			
1.3.6 Stateful Inspection (dynamic packet filtering) 을 적용한다. (즉, 이미 "체결된" 접속만 네트워크로 허용한다.)	1.3.6 방화벽이 stateful inspection (dynamic packet filtering)을 수행하는지 확인한다. [체결된 접속만 허용하며, 이전에 체결된 세션과 연관되어 있을 경우에만 접속을 허용함 (모든 TCP 포트에 대해 "syn reset" 또는 "syn ack" 비트를 설정하여 포트 스캐너를 수행 – 반응이 있는 것은 이전에 체결된 세션의 일부분이 아니라 할지라도 패킷이 허락되어 통과한다는 것을 의미한다.)]			
1.3.7 데이터베이스를 DMZ 로부터 분리된 내부 네트워크 구간에 위치시킨다.	1.3.7 데이터베이스가 DMZ 로부터 분리된 내부 네트워크 구간에 위치하는지 확인한다.			
1.3.8 내부 주소가 인터넷 상에 변환되어 공개되는 것을 제한하기 위해 RFC 1918 주소 공간을 사용하여 IP 은폐를 구현한다. 네트워크 주소 변환(NAT) 기술을 사용한다. (예: 포트 주소 변환(PAT))	1.3.8 방화벽과 라우터 구성요소의 표본을 대상으로, 내부 네트워크으로 부터 인터넷으로 IP 주소의 브로드캐스트를 제한하기 위해 RFC1918 주소 공간을 사용한 NAT 혹은 기타 기술들을 사용하고 있는지 확인한다. (IP 은폐)			
1.4 회사 네트워크를 접근하는데 사용되고, 인터넷에 직접 연결 가능한 이동형 컴퓨터 그리고/또는 직원 소유의 컴퓨터(예:직원용 노트북 컴퓨터)에 개인 방화벽 소프트웨어를 설치한다.	1.4.a 회사 네트워크를 접속하는데 사용되고, 인터넷에 직접 연결 가능한 이동형 컴퓨터 그리고/또는 직원 소유의 컴퓨터(예: 직원용 노트북 컴퓨터)에 개인 방화벽 소프트웨어가 설치 및 실행되고 있는지 확인한다.			
	1.4.b 개인 방화벽 소프트웨어는 회사가 정한 표준으로 설정되어 있으며, 모바일 컴퓨터 사용자에 의해 변경할 수 없는지 확인한다.			

요구사항 2: 시스템 패스워드 및 기타 보안 파라미터에 벤더가 제공한 디폴트 값을 사용하지 않는다

악의적인 개인들(회사 내부 및 외부)은 벤더가 제공한 디폴트 패스워드와 기타 벤더 디폴트 설정값 등을 사용하여 시스템 침해를 시도한다. 이런 패스워드들과 설정값은 해커 커뮤니티 사이에 이미 잘 알려져 있으며 공개된 정보를 통해 쉽게 파악된다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
2.1 시스템을 네트워크에 설치하기 전에 벤더가 제공한 디폴트 값을 항상 변경한다. (예: 패스워드, SNMP Community String, 불필요한 계정 제거)	2.1 시스템 구성요소, 중요 서버 및 무선 AP 의 표본을 선정하고, 벤더가 제공하는 디폴트 계정과 패스워드를 사용하여 장비에 (시스템 관리자의 도움을 받아) 로그온을 시도하여 디폴트 계정과 패스워드가 변경되었는지 확인한다. (벤더 매뉴얼과 인터넷의 소스를 사용하여 벤더가 제공하는 계정/패스워드를 확보한다.)			
2.1.1 카드회원 데이터 환경에 연결되어 있거나 카드회원 데이터를 전송하는 무선 환경에 대해, 디폴트 무선 암호화 키, 패스워드, SNMP Community String 등을 포함하는 무선 밴더 디폴트 값을 변경한다. 무선 장비 보안 설정에는 인증 및 전송에 강력한 암호화 기술을 적용하여야 한다.	2.1.1 무선 환경에 대해 벤더 디폴트 설정 관련 아래 사항을 확인하고 모든 무선 네트워크는 강력한 암호화 메카니즘을 구현하여야 한다 (예: AES): ▪ 설치 시에 암호화 키는 디폴트 상태에서 변경되었으며 키를 알고 있는 사람이 퇴사하거나 직무 변경이 된 경우 변경됨 ▪ 무선 장비의 디폴트 SNMP community string 이 변경됨 ▪ AP 의 디폴트 패스워드가 변경됨 ▪ 무선 장비의 펌웨어가 인증 및 무선 네트워크 전송에 강력한 암호화를 지원하기 위해 갱신됨 (예, WPA/WPA2) ▪ 기타 보안 관련 무선 벤더 디폴트값			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
2.2 모든 시스템 구성요소들에 대한 설정 기준들을 수립한다. 이 기준들이 모든 알려진 보안취약점들을 다루고 있으며 업계가 인정하는 시스템 강화 기준과 일치해야 한다.	2.2.a 모든 종류의 시스템 구성요소들에 대한 회사의 시스템 설정 기준들을 점검하여 시스템 설정 기준들이 업계가 인정하는 강화 기준과 일치하는지 확인한다. (예: SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), Center for Internet Security (CIS)).			
	2.2.b 시스템 설정 기준이 아래 (2.2.1 – 2.2.4) 각 항목을 포함하고 하는지 확인한다.			
	2.2.c 신규 시스템을 설정할 때 시스템 설정 기준이 적용되는지 확인한다.			
2.2.1 서버당 하나의 주요 기능만 구현한다.	2.2.1 시스템 구성요소의 표본에 대하여, 서버당 하나의 주요 기능만이 구현되었는지 확인한다. 예를 들면, 웹 서버, 데이터베이스 서버 및 DNS 는 별도의 서버로 구현되어야 한다.			
2.2.2 필요하지 않으며 안전하지 않은 서비스와 프로토콜(장비의 해당 기능을 수행하는데 직접 필요하지 않은 서비스와 프로토콜)을 비활성화한다.	2.2.2 시스템 구성요소의 표본에 대하여, 활성화된 시스템 서비스, 데몬, 프로토콜을 검사한다. 필요하지 않거나 안전하지 않은 서비스나 프로토콜이 활성화 되어 있지 않은지, 또는 해당 서비스의 사용에 대한 근거가 명확하게 문서화되어 있는지 확인한다. 예를 들면, FTP 가 사용되고 있지 않거나 SSH 나 다른 기술을 통해서 암호화 되어 있다.			
2.2.3 오용을 방지하기 위해 시스템 보안 파라미터를 설정한다.	2.2.3.a 인터뷰를 통해 시스템 관리자나 보안 관리자가 시스템 구성요소의 일반적인 보안 파라미터 설정에 대한 지식을 가지고 있는지 확인한다.			
	2.2.3.b 시스템 설정 기준에 일반적인 보안 파라미터 설정 내용이 포함되어 있는지 확인한다.			
	2.2.3.c 시스템 구성요소의 표본에 대하여, 일반적인 보안 파라미터가 적절하게 설정되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
2.2.4 스크립트, 드라이버, 기능, 하위 시스템, 파일 시스템, 불필요한 웹 서버 등과 같은 모든 불필요한 기능을 삭제한다.	2.2.4 시스템 구성요소의 표본에 대하여, 모든 불필요한 기능(스크립트, 드라이버, 기능, 하위시스템, 파일 시스템 등)이 제거되어 있는지 확인한다. 활성화된 기능들은 문서화되어 있으며, 안전한 설정을 지원하고 있는지, 문서화된 기능만 표본 장비에 존재하는지 확인한다.			
2.3 콘솔상에서의 접근이 아닌 경우 암호화한다. 웹기반 관리 및 콘솔 이외의 관리 접근에 대해 SSH, VPN 또는 SSL/TLS 등 기술을 사용한다.	2.3 시스템 구성요소의 표본에 대하여, 콘솔이 아닌 곳에서의 관리상 접속 시 다음 방식에 의해 암호화되어 있는지 확인한다. ▪ 관리자가 각 시스템에 로그 온 하는 것을 관찰하여 관리자 패스워드 요청전에 강력한 암호화 방법이 적용되는지 확인한다. ▪ 시스템의 서비스와 파라미터 파일을 검토하여 내부적으로 Telnet 및 기타 원격 로그인 명령어의 사용이 금지되고 있는지 확인한다. ▪ 웹기반 관리 인터페이스에 대한 관리자 접근에 강력한 암호화 방법이 사용되는지 확인한다.			
2.4 공유 호스팅 제공업체는 반드시 각 사업체의 호스팅 환경과 카드회원 데이터를 보호해야 한다. 제공업체는 반드시 "부록 A: 공유 호스팅 제공업체를 위한 추가 PCI DSS 요구사항"에 명시된 요구사항들을 만족시켜야 한다.	2.4 공유 호스팅 제공업체에 대한 PCI DSS 평가를 위해 "부록 A: 공유 호스팅 제공업체를 위한 추가 PCI DSS 요구사항"에 명시된 A.1.1 부터 A.1.4 의 시험 절차를 수행하여 공유 호스팅 제공업체가 각 사업체(가맹점과 서비스 제공업체)의 호스팅 환경과 데이터를 보호하고 있는지 확인한다.			

카드회원 데이터 보호

요구사항 3: 저장된 카드회원 데이터를 보호한다.

암호화, 잘라내기(truncation), 마스킹(masking), 그리고 해싱(hashing) 같은 보호 방법들은 카드회원 데이터 보호를 위해 매우 중요한 요소이다. 침입자가 다른 네트워크 보안 통제를 뚫고 암호화된 데이터에 접근한다 하더라도 해당 암호화 키가 없이는 데이터를 읽을 수도 없고 사용할 수도 없다. 저장된 데이터를 보호하는 다른 효과적인 방법들도 효과적인 위험 감소 수단으로 고려해 보아야 한다. 예를 들어, 위험을 감소시키는 방법으로는 반드시 필요한 경우가 아니면 카드회원 데이터를 저장하지 않기, PAN 전체가 필요하지 않으면 카드회원 데이터의 일부분을 잘라내기, 암호화된 이메일을 통해서만 PAN 전송하기가 포함된다.

"강력한 암호화" 및 기타 PCI DSS 용어의 정의는 "PCI DSS 용어집"을 참조한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.1 카드회원 데이터 저장을 최소로 유지해야 한다. 데이터 보유 및 폐기 정책을 수립해야 한다. 데이터 보유 정책에 문서화된 내용에 따라 사업적, 법적, 제도적 요구사항에 부합하는 저장 용량과 데이터 보유기간을 제한해야 한다.	3.1 회사의 데이터 보유 및 폐기 정책과 절차를 점검하여 다음을 수행한다: • 정책과 절차에, 카드회원 데이터 보유의 구체적 요구사항을 포함하여, 데이터 보존에 대한 법/제도/업무 요구사항을 포함하고 있는지 확인한다. (예, 카드회원 데이터는 Y 와 같은 사업적 이유로 X 기간 동안 보관되어야 함) • 정책과 절차에, 카드회원 데이터의 폐기를 포함하여, 법/제도/업무상 더 이상 필요하지 않은 데이터의 처분을 위한 조항을 포함하고 있는지 확인한다. • 정책과 절차가 저장되는 모든 카드회원 데이터를 범위로 포함하고 있는지 확인한다. • 정책과 절차에 최소한 분기별로 사업상 보관 기한을 넘긴 카드회원 데이터를 삭제하는 프로그램화된 (자동적인) 프로세스. 혹은 최소한 분기별로 카드회원 데이터가 업무상 필요한 보관 기한을 초과하여 보관되고 있는지를 검토하는 요구사항을 포함하고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.2 승인 이후에 중요한 인증 데이터를 저장하지 않는다. (암호화 여부와 관계 없음) 중요한 인증 데이터는 다음의 요구사항 3.2.1 부터 3.2.3 까지 언급된 데이터를 포함한다.	3.2 중요한 인증 데이터를 수신하여 삭제한 경우, 데이터 삭제 프로세스를 검토하여 이러한 데이터가 복구 불가능한지 확인한다. 아래의 중요한 인증 데이터에 대해 다음과 같은 단계를 수행한다:			
3.2.1 마그네틱 선 (카드 뒷면 또는 칩 혹은 다른 곳에 위치) 상의 어떠한 트랙이라도 전체 내용을 저장하면 안된다. 이러한 데이터는 full track, track, track 1, track 2, 마그네틱선 데이터 등으로 통칭된다. 주: 일반적인 업무 과정에서 마그네틱 선의 다음 데이터 항목들은 보존할 필요가 있을 수 있음: • 카드회원 이름 • 카드번호 (PAN) • 유효기간 • 서비스 코드 위험을 최소화하기 위해 이러한 데이터는 업무상 필요할 경우에만 저장한다. *주: 추가적인 정보는 "PCI DSS 용어집"을 참조하라.*	3.2.1 시스템 구성요소의 표본에 대하여, 아래 사항을 점검하여 카드 뒷면 마그네틱 상의 어떠한 트랙이라도 전체 내용을 절대로 저장하지 않고 않은지 확인한다: • 수신중인 거래 데이터 • 모든 로그 (예: transaction, history, debugging, error) • History files • Trace files • 몇몇의 데이터베이스 스키마 • 데이터베이스 내용			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.2.2 비대면(card-not-present) 거래를 확인하는데 사용되는 카드 확인 코드 또는 값 (카드 앞면이나 뒷면에 인쇄된 세 자리 또는 네 자리 값)을 저장하면 안 된다. *주: 추가적인 정보는 "PCI DSS 용어집"을 참조하라.*	3.2.2 시스템 구성요소의 표본에 대하여, 다음 사항을 점검하여 카드의 앞면이나 서명란에 인쇄된 세 자리 또는 네 자리의 카드 확인 코드 또는 값 (CVV2, CVC2, CID, CAV2 데이터) 을 절대로 저장하지 않고 있는지 확인한다: • 수신중인 거래 데이터 • 모든 로그 (예: transaction, history, debugging, error) • History files • Trace files • 몇몇의 데이터베이스 스키마 • 데이터베이스 내용			
3.2.3 개인 식별 번호 (PIN) 또는 암호화된 PIN 블록을 저장하면 안 된다.	3.2.3 시스템 구성요소의 표본에 대하여, 다음 사항을 점검하여 PIN 또는 암호화된 PIN 블록을 절대로 저장하지 않고 있는지 확인한다: • 수신중인 거래 데이터 • 모든 로그 (예: transaction, history, debugging, error) • History files • Trace files • 몇몇의 데이터베이스 스키마 • 데이터베이스 내용			
3.3 카드번호의 출력 시 마스킹 한다. (처음의 6 자리 숫자와 마지막 4 자리 숫자만 보여질 수 있는 최대 자리수임) *주:* *• 이 요구사항은 전체 PAN 을 봐야하는 정당한 업무상 필요성이 있는 직원과 기타 당사자에게는 적용되지 않는다.* *• 이 요구사항은 카드회원 데이터의 표시에 관한 보다 강화된 요구사항을 대체하지 않는다. 예를 들어, POS 영수증.*	3.3 문서화된 정책과 PAN 출력 내용(예: 스크린, 종이 영수증)을 점검하여, 정당한 업무 필요에 따라 전체 PAN 을 봐야하는 사람을 제외하고, 카드회원 데이터를 표시할 때 카드번호가 마스킹 되는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.4 카드번호는 어떤 곳에 저장(이동식 디지털 매체, 백업 매체, 로그) 되어 있더라도 다음과 같은 방법 중 하나를 이용하여 읽을 수 없는 형태로 되어야 한다: • 강력한 암호화 기반의 단방향 해쉬 • 잘라내기 (Truncation) • index token 과 pad (pad 는 안전한 곳에 저장되어야 함) • 강력한 암호화 및 관련 키 관리 프로세스와 절차 읽을 수 없도록 해야 하는 **최소한의** 계정 정보는 PAN 이다. *주:* *• 특정 사유로 회사가 PAN 을 읽을 수 없도록 하지 못하면, "부록 B: 보완 통제"를 참조한다.* *• "강력한 암호화"는 "PCI DSS 용어집"에 정의되어 있다.*	**3.4.a** PAN 을 보호하는 데 사용된 시스템 관련 문서를--(해당되는 경우) 공급업체, 시스템/프로세스의 유형, 암호화 알고리즘 포함--입수하여 점검한다. PAN 이 다음 방법들 중 한가지 방법을 사용하여 읽혀질 수 없도록 되어 있는지 확인한다: • 강력한 암호화 기반의 단방향 해쉬 • 잘라내기 (Truncation) • index token 과 pad (pad 는 안전한 곳에 저장되어야 함) • 강력한 암호화 및 관련 키 관리 프로세스와 절차			
	3.4.b 데이터 저장소 표본 중에서 일부 테이블 혹은 파일을 점검하여 PAN 을 읽을 수 없도록 되어 있는지--즉, 평문으로 저장되어 있지 않은지--확인한다.			
	3.4.c 이동 매체의 표본--예, 백업 테이프--을 점검하여 PAN 이 읽을 수 없도록 되어 있는지 확인한다.			
	3.4.d 감사로그의 표본을 점검하여 로그에서 PAN 이 가공되거나 삭제되어 있는지 확인한다.			
3.4.1 (파일이나 컬럼 레벨 데이터베이스 암호화가 아닌) 디스크 암호화가 사용되고 있다면 논리적인 접근은 반드시 기본 운영시스템 접근 통제 메커니즘과 독립적으로 관리되어야 한다. (예, 로컬 사용자 계정 데이터베이스를 사용하지 않음) 복호화 키는 사용자 계정에 같이 묶여 있으면 안 된다.	**3.4.1.a** 디스크 암호화가 사용된다면, 암호화된 파일 시스템으로의 논리적 접근은 기본 운영체제 메커니즘과 분리된 메커니즘을 통하여 구현되어 있는지 확인한다. (예: 로컬 사용자 계정 데이터베이스를 사용하지 않음)			
	3.4.1.b 암호화 키가 안전하게 저장되어 있는지 확인한다. (예: 강력한 접근 통제로 보호된 이동식 매체에 저장)			
	3.4.1.c 모든 이동식 미디어에 저장된 카드회원 데이터가 암호화되어 있는지 확인한다. *주: 디스크 암호화는 종종 이동식 매체를 암호화하지 못하기 때문에 이 매체에 저장된 데이터는 별도로 암호화할 필요가 있다.*			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.5 카드회원 데이터의 암호화에 사용된 암호화 키는 노출 또는 오용으로부터 보호한다.	3.5 카드회원 데이터의 암호화에 사용된 암호화 키를 노출 또는 오용으로부터 보호하는 프로세스를 다음과 같이 확인한다:			
3.5.1 암호화 키에 대한 접근을 필요한 최소한의 관리자로 제한한다.	3.5.1 사용자 접근 리스트를 점검하여 암호화 키에 대한 접근이 최소한의 관리자에게만 제한되어 있는지 확인한다.			
3.5.2 암호화 키를 최소한의 장소와 형태로 안전하게 저장한다.	3.5.2 시스템 구성 파일을 점검하여 키가 암호화된 형태로 저장되어 있으며, 키-암호화 키 (key-encrypting keys) 가 데이터-암호화 키 (data-encrypting keys) 와 분리되어 저장되어 있는지 확인한다.			
3.6 카드회원 데이터의 암호화에 사용된 암호화 키에 대한 모든 키 관리 프로세스와 절차를 다음 사항을 포함하여 문서화하고 적용한다:	3.6.a 카드회원 데이터의 암호화에 사용된 키에 대해서 키 관리 절차가 존재하는지 확인한다. *주: 키 관리를 위한 다양한 업계 기준을 NIST (http://csrc.nist.gov) 등 여러 자료에서 찾아볼 수 있다.*			
	3.6.b 서비스 제공업체에게만 해당됨: 서비스 제공업체가 카드회원 데이터의 전송을 위해 키를 고객과 공유하는 경우, 서비스 제공업체가 고객에게 키의 안전한 저장 및 변경 방법 등에 관한 가이드를 고객에게 제공하고 있는지 확인한다.			
	3.6.c 키 관리 절차를 점검하여 다음 사항을 확인한다:			
3.6.1 강력한 암호화 키 생성	3.6.1 강력한 키의 생성을 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			
3.6.2 암호화 키의 안전한 배포	3.6.2 안전한 키 배포를 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			
3.6.3 암호화 키의 안전한 저장	3.6.3 안전한 키 저장을 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
3.6.4 정기적으로 암호화 키 변경 • Re-keying 등과 같이 관련된 어플리케이션에 의해 필요하여 권고되는 사항 준수; • 최소 매년 실시	3.6.4 최소한 매년 키 변경을 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			
3.6.5 훼손 의심되거나 구(舊) 암호화 키의 회수 혹은 교체	3.6.5.a 구(舊) 키의 회수를 요구하도록 키 관리 절차가 적용되어 있는지 확인한다. (예: 해당하는 대로 보존, 파기, 말소)			
	3.6.5.b 훼손이 인지 혹은 의심되는 키의 교체를 요구하도록 키 관리 관리 절차가 적용되어 있는지 확인한다.			
3.6.6 암호화 키를 다수가 나누어 알고 이중 통제	3.6.6 키를 다수가 나누어 알고 이중 통제하도록 요구하게 키 관리 절차가 적용되어 있는지 확인한다 (예: 2~3 명의 관리자가 자신의 키만 알고 이들이 모두 모여야 전체 키를 재구성할 수 있음).			
3.6.7 암호화 키의 무승인 교체 예방	3.6.7 키의 무승인 교체 예방을 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			
3.6.8 암호화 키 관리자가 키 관리자 책임을 이해하고 수용함을 명시하는 양식에 서명 요구사항	3.6.8 키 관리자가 그들의 키 관리자 책임을 이해하고 수용함을 명시한 양식에 서명을 요구하도록 키 관리 절차가 적용되어 있는지 확인한다.			

요구사항 4: 공중망을 통한 카드회원 데이터를 암호화하여 전송한다.

악의를 가진 개인들이 쉽게 접근할 수 있는 네트워크로 전송되는 민감한 정보는 암호화 되어야 한다. 악의를 가진 개인들은 잘못 설정된 무선 네트워크와 기존 암호화 및 인증 프로토콜의 취약점들을 지속해서 목표로 삼아 카드회원 데이터 환경에 대한 접근 권한을 획득하기 위해 이러한 취약점들을 활용하게 된다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
4.1 공중망을 통해 전송되는 민감한 카드회원 데이터를 보호하기 위해 강력한 암호화와 함께 SSL/TLS, IPSEC 등과 같은 보안 프로토콜을 사용한다. PCI DSS 의 범위에 속하는 공중망의 예는: • 인터넷, • 무선 기술, • GSM (Global System for Mobile communications), • GPRS (General Packet Radio Service)	**4.1.a** 공중망을 통해 카드회원 데이터를 송수신되는 곳에서는 암호화--예를 들어, SSL/TLS 또는 IPSEC--의 사용을 확인한다. ▪ 데이터의 전송 중 강력한 암호화가 사용되고 있는지 확인한다. ▪ SSL 적용시: - 서버가 최신 패치 버전을 지원하는지 확인한다. - 브라우저 URL 의 일부에 HTTPS 가 나타나는지 확인한다. - URL 에 HTTPS 가 나타나지 않은 경우 카드회원 데이터를 요구하지 않는지 확인한다. ▪ 수신된 거래 표본을 선택하고 거래를 관찰하여 카드회원 데이터가 전송 중 암호화되어 있는지 확인한다. ▪ 오직 신뢰되는 SSL/TLS 키/인증서만 허용하는지 확인한다. ▪ 사용되고 있는 암호화 방법에 있어서 적정한 암호화 강도가 적용되었는지 확인한다. (벤더 권고사항 및 best practices 체크)			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
4.1.1 카드회원 데이터를 전송하거나 카드회원 데이터 환경에 연결된 무선 네트워크는 인증 및 전송에 강력한 암호화를 적용하기 위해 업계 best practice--예를 들어, IEEE 802.11i--를 사용한다. • 신규 무선환경 구현 시, 2009 년 3 월 31 일 이후에 WEP 를 구현하는 것은 금지된다. • 현행 무선환경에 대해서는, 2010 년 6 월 30 일 이후에 WEP 를 사용하는 것은 금지된다.	**4.1.1** 카드회원 데이터를 전송하거나 카드회원 데이터 환경에 연결된 무선 네트워크에 대해서 인증 및 전송에 강력한 암호화를 적용하기 위해 업계 best practices--예를 들어, IEEE 802.11i--를 사용하고 있는지 확인한다.			
4.2 일반 사용자 메시지 기술--예를 들어, e-mail, instant messaging, chat--에 의해 암호화되지 않은 PAN 을 전송하면 안 된다.	**4.2.a** 카드회원 데이터를 일반 사용자 메시지 기술을 통해 발송할 때마다 강력한 암호화가 사용되는지 확인한다.			
	4.2.b 암호화되지 않은 PAN 이 일반 사용자 메시지 기술을 통해 전송하지 않도록 명시한 정책이 존재하는지 확인한다.			

취약점 관리 프로그램 유지관리

요구사항 5: 안티바이러스 소프트웨어를 사용하고 정기적으로 갱신한다.

악성 소프트웨어--바이러스, 웜, 트로이목마를 포함--가 다양한 업무 활동--직원 이메일 및 인터넷/모바일 컴퓨터/저장 매체의 사용--중에 네트워크에 침입하여 시스템 취약점들을 악용하게 된다. 현재 및 발생하는 악성 소프트웨어 위협으로부터 시스템을 보호하기 위해 악성 소프트웨어에 일반적으로 영향을 받는 모든 시스템에는 안티바이러스 소프트웨어를 사용해야 한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
5.1 악성 소프트웨어에 의해 영향을 받는 모든 시스템--특히 개인용 컴퓨터와 서버들--에 안티바이러스 소프트웨어를 적용한다.	5.1 악성 소프트웨어에 의해 일반적으로 영향을 받는 모든 운영 시스템 종류를 포함하는 시스템 구성요소의 표본에 대해, 적용 가능한 안티 바이러스 기술이 존재할 경우 안티바이러스 소트웨어가 적용되어 있는지 확인한다.			
5.1.1 모든 안티바이러스 프로그램은 모든 알려진 종류의 악성 소프트웨어를 탐지, 삭제 및 방어할 수 있어야 한다.	5.1.1 시스템 구성요소의 표본에 대하여, 모든 안티바이러스 프로그램은 모든 알려진 종류의 악성 소프트웨어--예를 들어, 바이러스, 트로이 목마, 웜, 스파이웨어, 에드웨어, 루트킷--를 탐지, 삭제 및 방어하는지 확인한다.			
5.2 모든 안티바이러스 시스템이 최신의 상태로 작동하고 있으며, 감사 로그를 생성할 수 있어야 한다.	5.2 모든 안티 바이러스 소프트웨어가 최신의 상태로 작동하고 있으며, 로그를 생성할 수 있는지 다음과 같이 확인한다:			
	5.2.a 정책을 검토하여 안티 바이러스 소프트웨어 및 정의를 갱신하도록 요구하고 있는지 확인한다.			
	5.2.b 소프트웨어의 마스터 설치본이 자동 갱신 및 정기적 스캔을 활성화 하고 있는지 확인한다.			
	5.2.c 악성 소프트웨어에 의해 일반적으로 영향을 받는 모든 운영 시스템 종류를 포함하는 시스템 구성요소 표본에 대하여, 자동 갱신과 정기적인 스캔이 활성화 되어있는지 확인한다.			
	5.2.d 시스템 구성요소의 표본에 대하여, 안티바이러스 소프트웨어 로그 생성이 활성화되어 있고, 이러한 로그는 PCI DSS 요구사항 10.7 에 따라 보관되고 있는지 확인한다.			

요구사항 6: 안전한 시스템과 어플리케이션을 개발하고 유지한다.

부도덕한 사람들은 보안 취약점을 악용하여 시스템의 특수 접근권한을 획득한다. 대부분의 취약점들은 벤더가 제공한 보안 패치를 통해 교정되며, 시스템을 관리하는 사업체는 이 패치를 설치해야 한다. 모든 중요 시스템들에는 적절한 최신의 소프트웨어 패치를 적용하여 악의적인 개인들과 악성 소프트웨어로부터 카드회원 데이터에 대한 침해로부터 보호해야 한다.

주: 소프트웨어 패치가 적절히 이루어지기 위해서는 패치가 기존의 보안 설정과 충돌하지 않는지 확인하기 위해 충분히 평가 및 테스트되어야 한다. 자체 개발된 어플리케이션의 경우, 표준 시스템 개발 절차 및 보안 코딩 기술을 활용하여 취약점의 상당 부분을 해결할 수 있다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.1 모든 시스템 구성요소와 소프트웨어는 벤더가 제공하는 최신의 보안 패치를 설치해야 한다. 중요한 보안 패치는 발표된지 한달 이내에 설치되어야 한다. *주: 회사는 패치 설치의 우선 순위를 결정하기 위해 위험-기반 접근방법의 적용을 고려할 수 있다. 예를 들면, 중요 인프라--예를 들어, 인터넷용 장비 및 시스템, 데이터베이스--의 우선 순위를 덜 중요한 내부 장비보다 높게 결정하여, 높은 우선 순위의 시스템 및 장비는 1 개월 이내에, 덜 중요한 장비 및 시스템은 3 개월 이내에 다루어지게 할 수 있다.*	6.1.a 시스템 구성요소와 관련 소프트웨어의 샘플에 대하여, 각 시스템에 적용된 보안 패치 리스트와 최신 벤더가 제공한 보안 패치 리스트를 비교하여 최신의 벤더 패치가 설치되어 있는지 확인한다.			
	6.1.b 보안 패치와 관련된 정책을 점검하여 중요한 새로운 보안 패치가 발표된 지 한달 이내에 적용되어야 한다는 규정이 있는지 확인한다.			
6.2 새롭게 발견된 보안 취약점을 식별하는 프로세스를 수립한다. 예를 들어, 인터넷을 통해 무료로 제공되는 경고 서비스에 가입한다. 새로운 취약점 이슈를 다루기 위해 PCI DSS 요구사항 2.2 에서 요구하는 바대로 설정 기준을 개정한다.	6.2.a 새로운 보안 취약점을 식별하도록 프로세스가 구현되어 있는지 확인하기 위해 담당자를 인터뷰한다.			
	6.2.b 새로운 취약점을 식별하는 프로세스에 보안 취약점 정보를 확보할 외부 소스를 활용하고, 새로운 취약점 이슈가 발견됨에 따라 요구사항 2.2 에서 검토된 시스템 설정 기준을 업데이트 하는 내용이 포함되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.3 PCI DSS--예를 들면, 안전한 인증 및 로그 기록--및 업계 Best Practice 에 따라 소프트웨어를 개발하고, 소프트웨어 개발 라이프 사이클에 걸쳐 정보보호 관련 사항을 통합해야 한다. 이러한 절차는 반드시 다음을 포함해야 한다:	6.3.a 문서화된 소프트웨어 개발 프로세스를 검토하여 소프트웨어 개발 프로세스가 업계 표준을 따르고 있으며, 라이프 사이클에 걸쳐 정보보호 관련 사항이 포함되어 있고, 소프트웨어 어플리케이션이 PCI DSS 에 따라 개발되고 있는지 확인한다.			
	6.3.b 문서화된 소프트웨어 개발 프로세스의 점검, 소프트웨어 개발자 인터뷰, 관련 데이터--네트워크 설정 문서, 운영 및 테스트 데이터 등--의 검토를 통하여 다음 사항을 확인한다:			
6.3.1 모든 보안 패치와 시스템 및 소프트웨어 설정 변경사항은 적용 전 반드시 테스트를 거쳐야 하며, 다음 및 기타 사항을 포함한다:	6.3.1 모든 변경사항--패치를 포함하여-은 실제 운영 시스템에 적용되기 전에 테스트 되어야 한다.			
6.3.1.1 모든 입력 값 검증 (cross-site scripting, injection flaws, malicious file execution 등을 예방하기 위해)	6.3.1.1 모든 입력 값 검증 (cross-site scripting, injection flaws, malicious file execution 등을 예방하기 위해)			
6.3.1.2 적절한 에러 처리 검증	6.3.1.2 적절한 에러 처리 검증			
6.3.1.3 안전한 암호화 저장 검증	6.3.1.3 안전한 암호화 저장 검증			
6.3.1.4 안전한 커뮤니케이션 검증	6.3.1.4 안전한 커뮤니케이션 검증			
6.3.1.5 적절한 역할기반 접근제어 (RBAC) 검증	6.3.1.5 적절한 역할기반 접근제어 (RBAC) **검증**			
6.3.2 개발/테스트와 운영 환경의 분리	6.3.2 운영 환경으로부터 개발/테스트 환경이 분리되어 있으며, 분리된 환경의 접근 제어를 구현한다.			
6.3.3 개발/테스트와 운영 환경 사이의 직무 분리	6.3.3 개발/테스트 환경에 할당된 인력과 운영 환경에 할당된 인력간에 직무가 분리 되어 있어야 한다.			
6.3.4 운영 데이터--실제 PAN--를 테스트 및 개발을 위해서 사용하지 않는다.	6.3.4 운영 데이터--실제 PAN--를 테스트 및 개발을 위해 사용하지 않거나, 사용 전에 가공한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.3.5 운영 시스템이 가동되기 전에 테스트 데이터와 계정의 제거	6.3.5 운영 시스템이 가동되기 전에 테스트 데이터와 계정을 제거한다.			
6.3.6 어플리케이션이 가동되거나 고객에게 배포되기 전에 개발 어플리케이션 계정, 사용자 ID, 패스워드 제거	6.3.6 시스템이 운영되거나 고객에게 배포되기 전에 개발 어플리케이션 계정, 사용자 ID, 패스워드를 제거한다.			
6.3.7 모든 잠재적인 코딩 취약점을 식별하기 위해 운영시스템이나 고객에게 배포되기 전에 개발 코드 리뷰 *주: 코드 리뷰를 위한 본 요구사항은 PCI DSS 요구사항 6.3 에서 요구되는 시스템 개발 라이프 사이클의 일부로서 모든 개발 코드--내부 및 인터넷용 코드 모두)에 적용된다. 코드 리뷰는 지식을 갖춘 내부 인원이나 제 3 자에 의해 수행될 수 있다. 웹 어플리케이션 역시, 만약 대중과 접하고 있다면, PCI DSS 요구사항 6.6 에 정의된 것처럼 구현 이후에 진행중인 위협과 취약점을 다루기 위해 추가적인 통제를 필요로 한다.*	6.3.7.a 정책을 점검하여 내부 어플리케이션에 대한 모든 개발 어플리케이션 코드 변경사항이 다음과 같이--수작업이나 자동화된 프로세스를 사용하여--검토되는지 확인한다: ▪ 코드 변경사항은 코드를 만든 작성자 외의 개인이나, 코드 검토 기법 및 안전한 코딩 실무에 대한 지식이 있는 개인에 의해 검토 ▪ 배포 이전에 적절한 조치를 적용 ▪ 코드 리뷰 결과는 배포 이전에 경영층에 의에 검토되고 승인			
	6.3.7.b 정책을 점검하여 웹 어플리케이션에 대한 모든 개발 어플리케이션 코드 변경사항이 다음과 같이--수작업이나 자동화된 프로세스를 사용하여--검토되는지 확인한다: ▪ 코드 변경사항은 코드를 만든 작성자 외의 개인이나, 코드 검토 기법 및 안전한 코딩 실무에 대한 지식이 있는 개인에 의해 검토 ▪ 코드 리뷰는 코드가 Open Web Security Project Guide 와 같은 안전한 코딩 지침에 따라 개발 ▪ 배포 이전에 적절한 조치를 적용 ▪ 코드 리뷰 결과는 배포 이전에 경영층에 의에 검토되고 승인			
	6.3.7.c 최근의 개발 어플리케이션 변경사항에 대한 표본을 선택하여 개발 어플리케이션 코드가 위의 6.3.7a 및 6.3.7b 에 따라 검토되었는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.4 시스템 구성요소에 대한 모든 변경사항은 변경관리 절차를 따른다. 절차는 다음 사항이 포함되어야 한다:	6.4.a 보안 패치의 적용 및 소프트웨어 변경과 관련한 회사 변경관리 절차를 검토하여 6.4.1 – 6.4.4 의 항목을 요구하고 있는지 확인한다.			
	6.4.b 시스템 구성요소 및 최근의 변경사항/보안 패치의 표본에 대하여, 해당 변경사항을 관련된 변경 통제 문서로 역추적한다. 점검한 각각의 변경사항에 대해, 다음과 같은 사항을 수행한다:			
6.4.1 변경의 영향에 대한 문서화	6.4.1 각 표본의 변경사항에 대해 변경관리 문서 내에 변경의 영향에 대한 내용이 포함되어 있는지 확인한다.			
6.4.2 적합한 부서 관리자의 승인	6.4.2 각 표본의 변경사항에 대해 적합한 부서 관리자의 승인이 존재하는지 확인한다.			
6.4.3 운영 기능 테스트	6.4.3 각 표본의 변경사항에 대해 운영 기능 테스트가 수행되는지 확인한다.			
6.4.4 복귀(back-out) 절차	6.4.4 각 표본의 변경사항에 대해 복귀(back-out) 절차가 마련되어 있는지 확인한다.			
6.5 모든 웹 어플리케이션--내외부 및 어플리케이션에 대한 웹 관리자 접근--을 Open Web Application Security Project 와 같은 안전한 코딩 가이드라인을 기반으로 개발한다. 소프트웨어 개발 프로세스에는 일반적으로 발생하는 코딩 취약점을 예방하기 위해 다음과 같은 내용을 포함한다: *주: 6.5.1 부터 6.5.10 에 열거된 취약점들은 PCI DSS v1.2 가 공표된 시점의 OWASP 지침 내용이다. 그러나, 만약 OWASP 지침이 갱신된다면, 다음 요구사항에 반드시 최신 버전이 사용되어야 한다.*	6.5.a 모든 웹 기반 어플리케이션에 대한 개발 프로세스를 검토한다. 프로세스에는 개발자들을 대상으로 안전한 코딩 기법에 대한 교육 이수를 규정하고 있으며, OWASP 가이드 (http://www.owasp.org)와 같은 지침을 기반으로 하고 있는지 확인한다.			
	6.5.b 개발자 표본을 대상으로 인터뷰를 수행하고 이들이 안전한 코딩 기법에 대한 지식이 있는지 증거를 확보한다.			
	6.5.c 웹 기반 어플리케이션에 대해서 다음과 같은 사항에 취약하지 않게 하는 프로세스가 적용되어 있는지 확인한다:			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.5.1 크로스 사이트 스크립팅 (XSS)	6.5.1 Cross-site scripting (XSS) (모든 매개변수를 추가하기 전에 검증한다.)			
6.5.2 인젝션 오류, 특히 SQL 인젝션. 또한 LDAP 과 Xpath 인젝션 오류뿐만 아니라 다른 인젝션 오류들도 고려해야 한다.	6.5.2 인젝션 오류, 특히 SQL 인젝션 (명령어 및 쿼리의 의미를 사용자 데이터가 수정할 수 없음을 확인하기 위해 입력을 검증한다.)			
6.5.3 악성 파일 실행	6.5.3 악성 파일 실행 (어플리케이션이 사용자로부터 파일 이름이나 파일을 받아들이지 않는다는 것을 확인하기 위해 입력을 검증한다.)			
6.5.4 불안전한 직접 객체 참조	6.5.4 불안전한 직접 객체 참조 (내부 객체 참조를 사용자에게 노출하지 않는다.)			
6.5.5 크로스 사이트 요청 변조 (CSRF)	6.5.5 크로스 사이트 요청 변조 (CSRF) (브라우저에 의해 자동으로 제출된 승인 증명 및 토큰에 응답하지 않는다.)			
6.5.6 정보 유출과 부적절한 에러 처리	6.5.6 정보 유출과 부적절한 에러 처리 (오류 메시지나 다른 방법에 의해 정보를 누출하지 않는다.)			
6.5.7 취약한 인증 및 세션 관리	6.5.7 취약한 인증 및 세션 관리 (사용자를 적절히 인증하고 계정 증명과 세션 토큰을 보호한다.)			
6.5.8 불안전한 암호화 저장	6.5.8 불안전한 암호화 저장 (암호화 오류를 예방한다.)			
6.5.9 불안전한 통신	6.5.9 불안전한 통신 (모든 인증과 민감한 통신의 적절한 암호화)			
6.5.10 URL 접근통제 실패	6.5.10 URL 접근통제 실패 (모든 URL 에 대하여 대한 표현계층과 비즈니스 로직에 대한 일관된 접근통제를 적용한다.)			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
6.6 인터넷용 웹 어플리케이션에 대해, 새로운 위협 및 취약점을 지속하여 다루고, 해당 어플리케이션들이 다음 중 하나의 방법을 사용하여 알려진 공격들로부터 보호되도록 한다: • 최소 연 1 회 및 모든 변경 시, 수작업 혹은 자동화된 어플리케이션 취약점 보안 측정 도구 혹은 방법을 통해 인터넷용 웹 어플리케이션을 검토한다. • 인터넷용 웹 어플리케이션 앞에 웹-어플리케이션 방화벽을 설치한다.	6.6 인터넷용 웹 어플리케이션에 대해, 다음 중 하나의 방법이 적용되고 있는지 확인한다: ▪ 인터넷용 웹 어플리케이션들이 (수작업이나 자동화된 취약점 보안 점검 툴 혹은 방법을 사용하여) 다음과 같이 검토되는지 확인한다: – 최소 연 1 회 – 모든 변경 이후 – 어플리케이션 보안을 전문으로 하는 조직에 의해 – 모든 취약점들이 조치되고 – 조치 이후 어플리케이션을 재평가한다. ▪ 웹-어플리케이션 방화벽이 웹-기반 공격을 탐지 및 방지하기 위해 인터넷용 웹 어플리케이션 앞에 적용되어 있는지 확인한다. *주: 검토자가 어플리케이션 보안을 전문으로 하고 개발 팀으로부터 독립되었음을 증명할 수 있다면, "어플리케이션 보안을 전문으로 하는 조직"은 서드-파티 회사나 내부 조직이 될 수 있다.*			

강력한 접근 통제 방안 수립

요구사항 7: 업무상 알 필요가 있는지에 따라 카드회원 데이터에 대한 접근을 제한한다.

중요 데이터를 권한이 있는 인력만 접근할 수 있도록 하기 위해, 알 필요와 직무 책임에 기초하여 접근을 제한하도록 시스템과 프로세스를 적용하여야 한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
7.1 시스템 구성요소와 카드회원 데이터에 대한 접근을 해당 접근이 필요한 직원으로만 제한한다. 접근 제한은 다음을 포함해야 한다:	7.1 데이터 통제에 대한 서면 정책을 입수하고 검토하여 정책에 다음 사항들이 통합되어 있는지 확인한다:			
7.1.1 사용자 ID 의 접근권한은 해당 직무 책임을 수행하는데 필요한 최소한의 권한으로 제한	7.1.1 사용자 ID 의 접근권한은 해당 업무 직무 책임을 수행하는데 필요한 최소한의 권한으로 제한되어 있는지 확인한다.			
7.1.2 권한 할당은 개별 직원의 직무 분류와 기능을 근거로 함	7.1.2 권한이 직무 분류와 기능을 근거로 하여 할당되고 있는지 확인한다("role-based access control" 혹은 RBAC 으로도 불리움)			
7.1.3 승인 서식에 권한을 명시하고 관리자가 서명함	7.1.3 모든 접근에는 승인 서식이 필요하고, 서식에 필요한 권한을 명시하며, 서식에 관리자가 서명을 하는지 확인한다.			
7.1.4 자동화된 접근통제 시스템의 구현	7.1.4 접근통제가 자동화된 접근통제 시스템을 통해 구현되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
7.2 다중 사용자를 가진 시스템 구성요소에 대해 알 필요를 기준으로 접근을 제한하고, 명시적으로 허용된 경우를 제외하고 “모두 거부(deny all)” 하도록 접근통제 시스템을 설정한다. 접근통제 시스템은 다음 사항을 포함해야 한다:	7.2 시스템 설정과 벤더 문서를 검토하여 접근통제 시스템에 다음과 같은 사항이 적용되어 있는지 확인한다:			
7.2.1 모든 시스템 구성요소를 포함	7.2.1 모든 시스템 구성요소들에 대해서 접근통제 시스템이 적용되어 있는지 확인한다.			
7.2.2 직무 분류와 기능을 기준으로 개인별 권한 할당	7.2.2 직무 분류와 기능을 기준으로 개인에게 권한을 할당하도록 접근통제 시스템이 설정되어 있는지 확인한다.			
7.2.3 기본적으로 “deny-all” 설정	7.2.3 접근통제 시스템은 기본적으로 "deny-all"로 설정되어 있는지 점검 *주: 일부 접근통제 시스템의 경우 구체적인 거부 규정을 작성하기 전에는 기본적으로 “allow-all”로 설정되어 있는 경우가 있음*			

요구사항 8: 컴퓨터에 접근하는 사용자별로 고유 ID 를 부여한다.

접근하는 개개인에 대한 고유 식별자(ID) 할당은 개개인의 행동을 유일하게 기록할 수 있게 한다. 그러한 기록이 적용되어 있을 경우, 주요 데이터와 시스템에 대해 수행된 행동들이 권한을 보유한 사용자에 의해 수행되었으며, 이들이 수행하였음을 알 수 있게 된다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
8.1 모든 사용자에게 고유 ID 를 할당한 후에 시스템 구성요소 혹은 카드회원 데이터에 대한 접근을 허용하여야 한다.	8.1 모든 사용자에게 고유 ID 를 할당하여 시스템 구성요소 혹은 카드회원 데이터에 접근하게 하는지 확인한다.			
8.2 고유한 ID 이외에, 모든 사용자를 인증하기 위해 적어도 다음 중 한가지 방법을 사용해야 한다: • 패스워드 혹은 패스프레이즈 • 2-Factor 인증(예를 들어, 토큰 장비, 스마트 카드, 생체인식, 또는 공개키)	8.2 카드회원 데이터 환경 접근에 대해서 고유 ID 와 추가적인 인증(예: 패스워드)을 사용하여 사용자를 인증하는지 확인하기 위해 다음을 수행한다 ▪ 사용하는 인증방법을 기술한 문서를 검토한다. ▪ 사용하는 각 유형의 인증 방법과 각 유형의 시스템 구성요소에 대해, 인증을 관찰하여 인증이 문서에 기술된 인증방법과 일치하게 동작하는지 확인한다.			
8.3 직원, 관리자, 제 3 자에 의한 네트워크로의 원격 접속--네트워크 외부로부터 출발한 네트워크 계층 접속--에는 2-Factor 인증을 적용한다. 다음과 같은 기술을 사용한다: 원격 인증과 dial-in 서비스(RADIUS); 토큰을 사용한 TACACS (terminal access controller access control system); 개인 인증서를 사용한 VPN (SSL/TLS 나 IPSEC 기반).	8.3 모든 원격 네트워크 접속에 대해 2-Factor 인증이 적용되었는지 확인하기 위해, 직원(예: 관리자)이 네트워크로 원격 접속하는 것을 관찰하여 패스워드와 추가적인 인증 조치(예: 스마트카드, 토큰, PIN)가 필요한지 확인한다.			
8.4 모든 패스워드에 대해 강력한 암호화--"PCI DSS 용어집"에 정의된--를 사용하여 모든 시스템 구성요소에서 전송 및 저장 시 읽을 수 없도록 처리한다.	8.4.a 시스템 구성요소의 표본에 대하여, 패스워드 파일을 점검하여 패스워드가 전송 및 저장 중에 읽을 수 없도록 되어 있는지 확인한다.			
	8.4.b 서비스 제공업체만 해당: 패스워드 파일을 점검하여 고객의 패스워드가 암호화되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
8.5 모든 시스템 구성요소에서 비고객 사용자와 관리자에 대한 사용자 인증과 패스워드 관리를 다음과 같이 적절히 수행하여야 한다:	8.5 절차를 검토하고 직원을 인터뷰하여 사용자 인증과 패스워드 관리 절차가 적용되고 있는지 다음과 같이 확인한다:			
8.5.1 사용자 ID, 증명 및 기타 식별 객체의 추가, 삭제, 수정을 통제한다.	8.5.1.a 관리자 및 일반 사용자를 포함하여 사용자 ID 표본을 선정한다. 각 사용자가 회사 정책에 따라 시스템을 사용하는 권한이 있는지 다음과 같이 확인한다: ▪ 각 ID 의 승인 서식을 검토한다. ▪ 표본 사용자 ID 들이 승인 서식과 일치하게 적용--명시된 권한만 부여하고 모든 서명이 획득--되어 있는지 승인 서식과 해당 시스템을 대조하여 확인한다.			
8.5.2 패스워드 재설정 전에 사용자 신원을 확인한다.	8.5.2 패드워드 절차를 검토하고 보안관리자를 관찰하여, 사용자가 전화, e-mail, 웹 등 직접 대면하지 않고 패스워드 재설정을 요청할 경우, 패스워드를 재설정하기 전에 사용자 신원을 확인하는지 확인한다.			
8.5.3 최초 패스워드는 사용자별로 고유하게 할당하고 최초 사용 후 즉시 변경한다.	8.5.3 패스워드 절차를 검토하고 보안관리자를 관찰하여, 새로운 사용자를 위한 최초의 패스워드가 사용자별로 고유하게 할당되고 최초 사용 후 변경되는지 확인한다.			
8.5.4 퇴사한 모든 사용자의 접근권한을 즉시 말소한다.	8.5.4 최근 6 개월간 퇴사한 직원의 표본을 선정하고, 현재 사용자 접근 목록을 검토하여 퇴사 직원의 ID 가 비활성화 되었거나 제거되었는지 확인한다.			
8.5.5 최소 90 일마다 접속이력이 없는 사용자 계정을 제거 또는 정지한다.	8.5.5 90 일 이상 접속이력이 없는 계정을 삭제하거나 정지시키고 있는지 확인한다.			
8.5.6 원격 유지보수를 위해 벤더가 사용하는 계정은 필요한 시간 동안만 사용 가능하게 한다.	8.5.6 시스템 구성요소 지원 및 유지보수를 위해 밴더에 의해 사용되는 모든 계정은 비활성화 되어 있으며 필요시에만 활성화 되고, 사용 중에는 모니터링이 되고 있는지 확인한다.			
8.5.7 카드회원 데이터에 접근할 수 있는 모든 사용자에게 패스워드 절차와 정책을 배포한다.	8.5.7 사용자 ID 의 표본 사용자를 인터뷰하여 회사의 패스워드 절차와 정책을 인지하고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
8.5.8 그룹/공유/공용의 계정 및 패스워드를 사용하지 않는다.	8.5.8.a 시스템 구성요소의 표본에 대하여, 사용자 ID 목록을 검토하여 다음 사항을 확인한다: ▪ 공용 사용자 ID 와 계정이 비활성화되거나 제거됨 ▪ 시스템 관리 혹은 다른 중요한 작업을 위한 공유 계정이 존재하지 않음 ▪ 모든 시스템 구성요소의 관리에 공유/공용 계정이 사용되지 않음			
	8.5.8.b 패스워드 정책/절차를 검토하여 그룹/공유 패스워드가 명시적으로 금지되어 있는지 확인한다.			
	8.5.8.c 시스템 관리자를 인터뷰 하여 그룹/공유 패스워드 요청이 있을지라도 그러한 요청이 거부되는지 확인한다.			
8.5.9 최소 90 일마다 사용자 패스워드를 변경한다.	8.5.9 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 사용자 패스워드를 최소 90 일마다 변경하도록 사용자 패스워드 파라미터가 설정되어 있는지 확인한다. 서비스 제공업체에게만 해당: 내부 프로세스 및 고객/사용자 문서를 검토하여 고객의 패스워드가 정기적으로 변경되어야 하고 언제 어떤 환경에서 패스워드가 변경되어야 하는지에 대한 가이드를 고객에게 제공하고 있는지 확인한다.			
8.5.10 최소 7 자리의 최소 패스워드 길이를 요구한다.	8.5.10 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 패스워드를 최소 7 자 이상으로 하도록 패스워드 파라미터가 설정되어 있는지 확인한다. 서비스 제공업체에게만 해당: 내부 프로세스 및 고객/사용자 문서를 검토하여 고객의 패스워드가 최소 길이 요건의 준수를 요구하고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
8.5.11 숫자와 영문자를 모두 포함한 패스워드를 사용한다.	8.5.11 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 패스워드는 숫자와 영문자를 모두 포함하도록 패스워드 파라미터가 설정되어 있는지 확인한다. 서비스 제공업체에게만 해당: 내부 프로세스 및 고객/사용자 문서를 검토하여 고객의 패스워드가 숫자와 영문자를 모두 포함해야 한다고 요구하고 있는지 확인한다.			
8.5.12 새로운 패스워드는 사용자가 사용했던 마지막 4 개의 어떠한 패스워드도 사용을 허용하지 않는다.	8.5.12 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 새로운 패스워드는 이전에 사용한 4 개의 패스워드와 똑같이 사용할 수 없도록 패스워드 파라미터가 설정되어 있는지 확인한다. 서비스 제공업체에게만 해당: 내부 프로세스 및 고객/사용자 문서를 검토하여 새로운 고객 패스워드가 이전의 4 개의 패스워드와 같은 패스워드를 사용할 수 없도록 하는지 확인한다.			
8.5.13 6 번 이상의 접근시도가 실패한 후 사용자의 ID 를 잠그도록 하여 반복된 접근시도를 제한한다.	8.5.13 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 6 번이 넘는 반복된 접근 시도 실패 시 해당 ID 를 잠그도록 패스워드 파라미터가 설정되어 있는지 확인한다. 서비스 제공업체에게만 해당: 내부 프로세스 및 고객/사용자 문서를 통해 6 번이 넘는 반복된 접근시도 실패 시 해당 ID 가 잠기는지 확인한다.			
8.5.14 잠금 시간을 최소 30 분 또는 관리자가 사용 ID 를 활성화 할 때까지로 설정한다.	8.5.14 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 일단 사용자 ID 의 사용이 중지되면 최소 30 분간 또는 관리자가 계정을 재설정 할 때까지 계정이 잠기도록 패스워드 파라미터가 설정되어 있는지 확인한다.			
8.5.15 세션이 15 분 이상 사용되지 않으면, 터미널을 재작동(re-activate) 하기 위해 사용자에게 패스워드를 다시 입력하도록 요구한다.	8.5.15 시스템 구성 요소의 표본에 대하여, 시스템 설정 내용을 점검하여 시스템/세션 idle time out 기능이 15 분 또는 그 이하로 설정되어 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
8.5.16 카드회원 데이터를 저장하고 있는 모든 데이터베이스로의 모든 접근에 대해 인증한다. 여기에는 어플리케이션, 관리자 및 다른 모든 사용자의 접근이 포함된다.	8.5.16.a 데이터베이스와 어플리케이션의 설정 내용을 검토하여 데이터베이스로의 사용자 인증과 접근에 다음 사항을 확인한다: ▪ 모든 사용자는 접근하기 전에 인증됨 ▪ 데이터베이스로의 모든 사용자의 접근, 질의 및 활동(예: move, copy, delete)은 프로그래밍 방식만을 허용함 (예: 저장 프로시저를 통해) ▪ 데이터베이스에 직접 접근 혹은 질의는 데이터베이스 관리자로 제한함			
	8.5.16.b 데이터베이스 어플리케이션과 관련 어플리케이션 ID 를 검토하여 어플리케이션 ID 는 오직 어플리케이션에 의해서만 사용될 수 있음--개별 사용자나 기타 프로세스에 의해 사용되지 않음-을 확인한다.			

요구사항 9: 카드회원 데이터에 대한 물리적 접근을 제한한다.

카드회원 데이터가 포함된 데이터나 시스템에 대한 모든 물리적 접근은, 개인으로 하여금 장비나 데이터에 접근하여 시스템이나 하드카피를 삭제하게 할 수 있으므로, 적절히 제한되어야 한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
9.1 적절한 시설 출입 통제를 사용하여 카드회원 데이터 환경 내의 시스템에 대한 물리적 접근을 제한하고 감시한다.	9.1 카드회원 데이터 환경 내의 각 컴퓨터실, 데이터 센터 및 시스템이 있는 기타 물리 공간에 대해 물리적 보안 통제가 존재하는지 확인한다. ▪ 배지 리더기나 기타 장치--출입증, 잠금장치/열쇠--들을 이용하여 접근이 통제되고 있는지 확인한다. ▪ 카드회원 데이터 환경에 위치한 시스템들을 임의로 선정하여 콘솔에 대한 시스템 관리자의 로그인 시도를 관찰하여, 비인가된 사용을 예방하기 위하여 "잠겨" 있는지 확인한다.			
9.1.1 비디오 카메라 혹은 기타 접근통제 메카니즘을 사용하여 민감한 구역에 대한 개인의 물리적 접근을 감시한다. 수집된 데이터를 검토하여 다른 출입기록과 대사를 한다. 법으로 제한되지 않는 한 최소 3 개월 동안 보관한다. *주: "민감한 구역"이란 카드회원 데이터를 저장, 처리 또는 전송하는 시스템이 입주한 데이터 센터, 서버실 혹은 구역을 지칭한다. 소매점 내의 계산 공간 같이 POS 터미널만 존재하는 곳은 제외한다.*	9.1.1 비디오 카메라 혹은 기타 접근통제 메커니즘이 적용되어 민감한 구역에 대한 출입구를 감시하고 있는지 확인한다. 비디오 카메라 혹은 기타 장치는 부당한 조작이나 작동불능으로부터 보호되어야 한다. 비디오 카메라나 기타 장치가 감시되는지 확인하고, 카메라 혹은 기타 장치의 데이터가 최소 3 개월 동안 보관되는지 확인한다.			
9.1.2 누구나 접근할 수 있는 네트워크 잭에 대한 물리적 접근을 제한한다.	9.1.2 네트워크 잭은 승인된 직원이 필요로할 때 만 사용이 가능한지 네트워크 관리자와의 인터뷰와 관찰로 확인한다. 예를 들어 방문자를 맞이하는 회의실과 같은 곳에 DHCP 로 사용 가능한 네트워크 포트가 존재하면 안 된다. 네트워크 잭이 존재하는 장소에는 방문자를 내부인이 함께 동행하는지 확인한다.			
9.1.3 무선 AP, 게이트웨이, 휴대용 장비에 대한 물리적 접근을 제한한다.	9.1.3 무선 AP, 게이트웨이 및 휴대용 장비에 대한 물리적 접근이 적절히 제한되고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
9.2 특히 카드회원 데이터에 접근할 수 있는 장소에서, 모든 인원들이 직원과 방문자로 쉽게 구분할 수 있도록 하는 절차를 개발한다. 본 요구사항에서 쓰이는, "직원"은 사업장에 상주하는 정규 직원, 비정규 직원, 임시고용직 및 계약자와 컨설턴트를 말한다. "방문자"는 하루를 넘기지 않는 짧은 기간 해당 시설에 출입해야 하는 벤더, 직원의 방문객, 서비스 직원 등을 말한다.	9.2.a 직원과 방문자에게 출입증을 발급하는 프로세스와 절차를 검토하고, 이 프로세스에 다음 내용이 포함되어 있는지 확인한다: ▪ 신규 출입증 발급, 접근 요구사항 변경, 퇴사 직원이나 유효기간이 지난 방문자 배지의 취소 ▪ 출입증 시스템에 대한 접근 제한			
	9.2.b 시설 내의 사람들을 관찰하여 직원과 방문자의 식별이 용이한지 확인한다.			
9.3 모든 방문자는 다음과 같이 통제한다:	9.3 직원/방문자 통제가 다음과 같이 적용되어 있는지 확인한다:			
9.3.1 카드회원 데이터를 처리하거나 유지하는 구역은 출입하기 전에 승인되어야 한다.	9.3.1 방문자를 관찰하여 방문자 ID 출입증을 사용하는지 확인한다. 을 위하여 방문자 관찰. 데이터 센터로의 접근을 시도하여 방문자 ID 배지로 담당자 동행 없이 카드회원 데이터가 저장되어 있는 물리적 장소로의 접근을 허용하지 않는지 확인한다.			
9.3.2 비임직원인 방문자를 식별하고, 기한이 만료되는 물리적 토큰--예: 출입증 또는 접근 장치--을 지급한다.	9.3.2 직원 및 방문자 출입증을 점검하여 ID 출입증이 방문자/외부자와 임직원을 명확히 구분하고, 기한이 만료되는지 확인한다.			
9.3.3 시설을 떠나거나 기한이 만료되었을 경우 물리적 토큰을 반납하도록 요청한다.	9.3.3 시설을 떠나는 방문자를 관찰하여 방문자가 떠나거나 기한이 만료되었을 경우 ID 출입증에 대한 반납 요청이 이루어지는지 확인한다.			
9.4 방문자 활동에 대한 물리적 감사 추적을 위하여 방문자 기록을 활용한다. 방문자의 이름, 재직중인 회사, 물리적 접근에 대한 직원 인증을 로그 상에 기록한다. 법에서 별도로 요구하지 않을 경우 최소 3 개월 동안 보관한다.	9.4.a 카드회원 데이터를 저장하거나 송수신하는 컴퓨터실, 데이터센터 및 관련 시설로의 방문자 기록이 남겨지는지 확인한다.			
	9.4.b 기록에는 방문자 이름, 소속 회사, 출입을 허락한 직원의 이름이 포함되며, 최소 3 개월 동안 보관하는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
9.5 대체 또는 백업 사이트, 또는 상업 스토리지 시설 같은 물리적으로 떨어진 안전한 장소에 백업 매체를 보관한다. 최소 연 1 회 해당 장소의 보안을 점검한다.	9.5 백업 매체 보관이 안전한지 확인하기 위해 최소 연 1 회 이상 저장소가 검토되는지 확인한다.			
9.6 카드회원 데이터를 담고 있는 모든 종이 및 전자 매체를 물리적으로 보호한다.	9.6 카드회원 데이터를 보호하는 절차가 종이 및 전자매체--컴퓨터, 이동 전자 매체, 네트워크 및 통신 하드웨어, 통신 회선, 종이 영수증, 종이 보고서, 팩스 포함--의 물리적 보호를 위한 통제를 포함하는지 확인한다.			
9.7 카드회원 데이터를 담고 있는 모든 종류의 매체의 내부/외부 배포에 대해 다음 사항을 포함하여 엄격히 통제한다:	9.7 카드회원 데이터를 담고 있는 매체의 배포를 통제하기 위한 정책이 존재하고, 해당 정책에는 모든 배포된 매체--개인에게 배포된 매체를 포함--를 포함하는지 확인한다.			
9.7.1 해당 매체가 기밀(confidential)로 식별되도록 분류한다.	9.7.1 해당 매체가 "기밀(confidential)"로 식별되도록 분류되었는지 확인한다.			
9.7.2 정확하게 추적이 가능한 안전한 배송업체나 기타 배달 방법을 이용하여 매체를 전달한다.	9.7.2 시설 외부로 보내는 모든 매체는 기록을 남기고 관리자의 승인을 받으며, 추적이 가능한 안전한 배송업체나 기타 배달 방법을 이용하여 전달하는지 확인한다.			
9.8 보안구역으로부터 옮겨진, 카드회원 데이터를 포함하는 모든 매체는 관리자의 승인을 받아야 한다. (특히 개인에게 매체가 배포되는 경우)	9.8 카드회원 데이터를 포함하는 모든 매체의 Offsite 이동 기록 중 최근 몇 일을 표본으로 선택하여, 상세한 추적 로그와 적정한 관리자의 승인이 존재하는지 확인한다.			
9.9 카드회원 데이터를 담고 있는 저장소나 매체의 접근에 대해 엄격히 통제한다.	9.9 매체 저장소 통제와 하드카피 및 전자 매체의 관리에 대한 정책을 점검하고, 해당 정책이 정기적인 매체 목록 조사를 규정하는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
9.9.1 모든 매체의 로그 목록을 적절히 유지하고 최소 연 1 회 매체 재고를 조사한다.	9.9.1 매체 목록 기록을 점검하여 최소 연 1 회 이상 정기적인 재고 조사가 이루어졌는지 확인한다.			
9.10 사업상 혹은 법적으로 더 이상 필요하지 않은 카드회원 데이터를 포함하고 있는 매체는 다음과 같이 파기한다:	9.10 정기적인 매체 파기 정책을 검토하여 해당 정책이 카드회원 데이터를 포함한 모든 매체를 포괄하는지 점검하고 다음의 내용을 확인한다:			
9.10.1 카드회원 데이터가 복구될 수 없도록 하드카피 자료의 절단, 소각 또는 펄프 처리한다.	9.10.1.a 하드카피 자료가 복구 될 수 없음을 합리적으로 보증할 정도로 하드카피 자료가 절단, 소각, 펄프 처리되는지 확인한다.			
	9.10.1.b 파기할 정보를 보관하는 컨테이너를 점검하여 컨테이너가 안전한지 확인한다. 예를 들어 "파기용" 컨테이너에 잠금장치를 설치하여 내용물로의 접근을 방지하는지 확인한다.			
9.10.2 카드회원 데이터가 복구될 수 없도록 전자 매체를 재생 불가능하게 한다.	9.10.2 안전한 삭제를 위해 산업용 표준에 따른 Security wipe 프로그램을 통해서나, 그렇지 않으면 매체를 물리적으로 파기(예를 들어, 자성 제거)하여, 전자 매체의 카드사용자 데이터를 재생 불가능 하게 한다.			

네트워크 정기적 모니터링 및 테스트

요구사항 10: 네트워크 자원과 카드회원 데이터에 대한 모든 접근을 추적하고 감시한다.

로깅 메커니즘 (Logging mechanism)과 사용자 활동 내역 추적 능력은 데이터 훼손의 예방, 발견, 또는 영향 최소화에 있어서 매우 중요하다. 모든 환경에 로그를 생성함으로써 문제 발생 시 이를 분석, 경고 그리고 추적할 수 있다. 시스템 활동 로그가 없이는 훼손의 원인을 찾기가 매우 어렵다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
10.1 시스템 구성요소에 대한 모든 접근 시도--특히 root 와 같은 관리자 권한을 통한 접근 시도--를 개별 사용자와 연관지을 수 있는 프로세스를 수립한다.	10.1 관찰과 시스템 관리자와의 인터뷰를 통하여, 시스템 구성요소에 대한 감사 추적이 가능하고 활성화되어 있음을 확인한다.			
10.2 다음 이벤트의 복원을 위하여 모든 시스템 구성요소들의 자동화된 감사 추적 기능을 구현한다.	10.2 인터뷰, 감사 로그 점검, 감사 로그 설정 점검을 통하여 다음 사항이 수행되고 있는지 확인한다.			
10.2.1 카드회원 데이터에 대한 모든 개별적 접근	10.2.1 카드회원 데이터에 대한 모든 개별적인 접근에 대해 로그가 기록되는지 확인한다.			
10.2.2 모든 개인이 root 혹은 관리자 권한을 통해 수행한 모든 조작	10.2.2 모든 개인이 root 혹은 관리자 권한을 통해 수행한 모든 조작에 대한 로그가 기록되는지 확인한다.			
10.2.3 감사 기록에 대한 접근	10.2.3 모든 감사 기록에 대한 접근에 대해 로그가 기록되는지 확인한다.			
10.2.4 잘못된 논리적 접근 시도	10.2.4 잘못된 논리적 접근 시도에 대해 로그가 기록되는지 확인한다.			
10.2 5 식별 및 인증 메커니즘의 사용	10.2.5 식별 및 인증 메커니즘의 사용에 대해 로그가 기록되는지 확인한다.			
10.2.6 감사 로그의 초기화	10.2.6 감사 로그 초기화에 대해 로그가 기록되는지 확인한다.			
10.2.7 시스템 레벨 객체의 생성 및 삭제	10.2.7 시스템 레벨 객체의 생성과 삭제에 대한 로그가 기록되는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
10.3 모든 시스템 구성요소들의 각각의 이벤트에 대해서 최소한 다음의 감사 항목들을 기록한다:	10.3 인터뷰와 관찰을 통하여 10.2 에서 언급된 감사 대상 이벤트와 관련하여 다음 사항들이 수행되고 있는지 확인한다.			
10.3.1 사용자 식별	10.3.1 사용자 식별이 로그 항목에 포함되는지 확인한다.			
10.3.2 이벤트 종류	10.3.2 이벤트 종류가 로그 항목에 포함되는지 확인한다.			
10.3.3 날짜와 시간	10.3.3 날짜와 시간 stamp 가 로그 항목에 포함되는지 확인한다.			
10.3.4 성공 혹은 실패 표시	10.3.4 성공 혹은 실패 표시가 로그 항목에 포함되는지 확인한다.			
10.3.5 이벤트의 시작지점	10.3.5 이벤트의 시작지점이 로그 항목에 포함되는지 확인한다.			
10.3.6 영향을 받는 데이터, 시스템 구성요소 또는 자원의 신원 또는 이름	10.3.6 영향을 받는 데이터, 시스템 구성요소 또는 자원의 신원 또는 이름이 로그 항목에 포함되는지 확인한다.			
10.4 모든 중요 시스템의 시간을 동기화 한다.	10.4 회사 내에서 정확한 시간을 획득하여 배포하는 프로세스를 검토하고, 시스템 구성요소의 표본에 대하여 시간 관련 시스템 변수들을 점검한다. 다음의 내용들이 프로세스에 포함되어 있으며, 적용되었는지 확인한다:			
	10.4.a PCI DSS 요구사항 6.1 과 6.2 와 같이, 안정된 버전의 NTP 또는 유사한 기술이 시간 동기화를 위하여 사용되는지 확인한다.			
	10.4.b 내부 서버들이 모두 외부 소스로부터 타임 신호를 받지 않는지 확인한다. [회사 내부의 2~3 대의 중앙 타임 서버들이 외부 소스[특별한 무선 라디오, GPS 위성으로부터 직접 받거나, 또는 국제원자시(IAT)와 UTC(과거 GMT)에 근거한 외부 소스]로부터 타임 신호를 받아서 서로 비교함으로써 정확한 시간을 맞추고, 다른 내부의 서버들과 시간을 공유한다.]			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
	10.4.c 타임서버가 NTP 타임 업데이트를 제공받을 수 있도록 (악의적인 개인에 의한 시각 변경 예방하기 위해) 특정 외부 호스트를 지정하였는지 확인한다. 선택사항으로는 이러한 업데이트는 (내부 타임 서버의 비인가된 사용 예방을 방지하기 위해) 대칭키로 암호화할 수 있으며, NTP 서비스를 제공받는 클라이언트 머신의 IP 주소를 명기하여 접근 통제 목록을 생성할 수 있다. 추가 정보는 www.ntp.org 를 참조한다.			
10.5 변경되어지지 않도록 감사 기록의 보호	10.5 시스템 관리자와의 인터뷰와 파일 권한 점검을 통하여 감사 기록이 변경되지 않도록 안전하게 보호되는지 확인한다.			
10.5.1 감사 기록의 열람을 업무와 관련된 자로 제한한다.	10.5.1 업무와 관련된 자만 감사 기록 파일을 열람할 수 있는지 확인한다.			
10.5.2 비인가된 변경으로부터 감사 기록 파일을 보호한다.	10.5.2 현재 감사 기록 파일이 접근통제 메카니즘, 물리적 분리, 그리고/또는, 네트워크 분리 등을 통하여 비인가자로부터 안전하게 보호되는지 확인한다.			
10.5.3 중앙집중화된 로그 서버 또는 변경이 어려운 매체로 감사 기록 파일을 즉시 백업한다.	10.5.3 감사 기록 파일이 중앙 집중화된 로그 서버나 변경이 어려운 매체로 즉시 백업되는지 확인한다.			
10.5.4 외부와 접하는 기술과 관련된 로그를 내부 LAN 의 로그 서버에 기록한다.	10.5.4 외부와 접하는 기술(예를 들어, 무선, 방화벽, DNS, 메일)과 관련된 로그를 Offload 하거나, 안전하게 중앙 집중화된 내부 로그 서버나 매체로 저장되는지 확인한다.			
10.5.5 존재하는 로그 데이터 파일이 경고 없이 변경되지 않도록 하기 위하여 로그 파일 무결성 모니터링 혹은 변경 탐지 소프트웨어를 사용한다. (새로운 데이터가 추가되는 경우는 경고가 필요하지 않음)	10.5.5 시스템 설정, 모니터한 파일, 모니터링 결과 등을 점검하여 감사 로그를 대상으로 파일 무결성 모니터링 또는 변경 탐지 소프트웨어를 사용하는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
10.6 모든 시스템의 로그는 최소한 매일 점검해야 한다. 로그 점검시 IDS 및 AAA 서버(예: RADIUS)와 같은 보안 시스템도 포함해야 한다. *주: 로그 수집, 분석, 경고 도구는 요구사항 10.6 을 준수하기 위해 사용이 가능하다.*	10.6.a 보안정책 및 절차를 검토하여 보안로그에 대한 점검을 매일 수행하고 있으며 예외사항에 대해 추적조사를 수행하도록 요구하고 하고 있는지 확인한다.			
	10.6.b 관찰과 인터뷰를 통하여, 모든 시스템에 대한 정기적인 로그 점검이 수행되고 있는지 확인한다.			
10.7 감사 기록 히스토리를 최소 1 년간 보관하며, 최소 3 개월 간은 분석을 위해 즉시 이용 가능하도록(예를 들어, 온라인이나, 보관소나, 백업으로부터 복구 가능한 상태로) 유지해야 한다.	10.7.a 보안 정책과 절차를 점검하여, 감사 로그 보관 정책이 존재하고, 최소 1 년 이상 보관하도록 규정하고 있는지 확인한다.			
	10.7.b 최소 1 년간의 감사 로그를 확인할 수 있는지, 그리고 즉시 분석 가능하도록 최소 지난 3 개월간의 로그를 복구하는 적절한 절차가 있는지 확인한다.			

요구사항 11: 보안시스템 및 프로세스를 정기적으로 시험한다.

취약점들이 악의적인 개인들 및 연구자에 의해 계속 발견되고 있으며, 또한 새로운 소프트웨어에 의해 나타나게 된다. 시스템 구성요소, 프로세스 및 개발 소프트웨어를 자주 테스트하여 보안 통제사항들이 변화하는 환경을 지속적으로 반영하여야 한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
11.1 최소 분기별 1 회 무선 분석 장치를 이용하거나 이용중인 모든 무선 장비를 식별해주는 무선 IDS/IPS 를 설치하여 무선 AP 가 존재하는지 테스트한다.	11.1.a 최소 분기별 1 회 무선 분석 장치가 사용되고 있는지, 모든 무선 장비를 식별하는 무선 IDS/IPS 가 구현 및 설정 되었는지를 확인한다.			
	11.1.b 무선 IDS/IPS 가 구현되었다면, 담당자에게 경보를 전달하도록 설정되었는지를 확인한다.			
	11.1 c 회사의 침해사고 대응 계획(요구사항 12.9)이 인증되지 않은 무선 장비를 탐지하였을 때의 대응을 포함하는지 확인한다.			
11.2 최소 분기당 한 번 혹은 네트워크에 중대한 변경이 발생했을 경우 내부 및 외부 네트워크에 대한 네트워크 취약점 스캐닝을 수행한다. (예: 새로운 시스템 자원 설치, 네트워크 구성도 변화, 방화벽 규정 변경, 제품 업그레이드) *주: 분기별 외부 취약점 스캐닝은 PCI SSC 의 인증을 받은 공인 스캐닝 업체(ASV)에 의해 수행되어야 한다. 네트워크가 변경된 이후의 스캐닝 관리는 내부 스탭에 의해 수행될 수 있다.*	11.2.a 최근 4 분기 동안의 네트워크/서버/어플리케이션 취약점 스캔과 관련된 산출물을 점검하여 카드회원 데이터를 관리하고 있는 환경에 대한 정기적인 보안 점검이 수행되고 있는지 확인한다. 스캔 프로세스에 결과값이 통과 될 때까지 스캔을 계속하는 과정이 포함되어 있는지 확인한다. *주: 네트워크 변경 이후에 수행되는 외부 스캔, 그리고 내부 스캔은 자격이 있는 회사 내부 인원이나 서드 파티에서 이행할 수 있다.*			
	11.2.b 외부 취약점 스캔 (external vulnerability scan) 이 PCI Security Scanning Procedures 와 일치하게 분기별로 이루어지고 있는지 점검하고, 최근 4 분기 동안의 산출물을 검사하여 아래 내용을 확인한다: ▪ 최근 12 개월간 분기별로 4 번의 스캔을 수행해야 함. 각 분기별 스캔 결과가 PCI Security Scanning Procedures 를 만족해야 함. (예: 시급(urgent), 심각(critical) 또는 높은(high) 수준의 취약점이 없어야 함) ▪ 취약점 스캔이 PCI SSC 의 인증을 받은 공인			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
	스캐닝 업체(ASV)에 의해 수행되어야 함. *주: 최초의 PCI DSS 준수인 경우, QSA 가 아래 내용 모두를 확인한다면, 4 번의 통과된 분기별 스캔이 필요한 것은 아니다. 1) 가장 최근의 스캔 결과가 통과되었고, 2) 사업체가 분기별 스캐닝을 요구하는 문서화된 정책 및 절차를 보유하고 있으며, 3) 스캔 결과에 기록된 취약점들이 다시 스캔한 결과 교정되었다. 최초의 PCI DSS 검토 이후, 다음 연도는 분기별로 4 번의 스캔이 반드시 이루어져야 한다.*			
	11.2.c 최근 연도의 스캔 결과를 점검하여, 네트워크에 어떤 중요한 변화가 발생한 이후에 내부 및/혹은 외부 스캐닝이 수행되었는지를 확인한다. 스캔 프로세스에 결과값이 통과될 때까지 스캔을 계속하는 과정이 포함되어 있는지 확인한다.			
11.3 외부 및 내부 침투시험을 적어도 매년 수행하고, 인프라와 어플리케이션을 대폭 업그레이드하거나 변경한 후--예: OS 업그레이드, 대상 환경에 서브 네트워크의 추가, 또는 대상 환경에 웹 서버의 추가에도 수행한다.	**11.3.a** 가장 최근의 침투시험 결과를 입수 및 점검하여, 침투시험을 적어도 매년 수행하며, 대상 환경에 대폭적인 변경이 발생한 이후에도 수행하는지 확인한다. 파악된 취약점이 해결되었으며 시험이 반복되었는지 확인한다.			
	11.3.b 침투시험이 자격을 갖춘 내부 인력이나 자격을 갖춘 외부의 서드 파티에 의해서 수행되었는지, 그리고 해당할 경우, 침투시험 수행자--QSA 나 ASV 일 필요는 없음--가 대상 조직으로부터 독립성을 갖는지 확인한다.			
11.3.1 네트워크 계층 침투시험	**11.3.1** 침투시험이 네트워크 계층의 침투시험을 포함하는지 확인한다. 시험에는 운영 체제는 물론 네트워크 기능을 지원하는 구성 요소를 포함해야 한다.			
11.3.2 어플리케이션 계층 침투시험	**11.3.2** 침투시험이 어플리케이션 계층의 침투시험을 포함하는지 확인한다. 웹 어플리케이션의 경우, 테스트는, 최소한, 요구사항 6.5 에 나열된 취약점을 포함해야 한다.			
11.4 IDS(intrusion detection systems) 및/혹은 IPS(intrusion prevention systems)를 사용하여	**11.4.a** IDS 및/혹은 IPS 를 사용하고 카드회원 데이터 환경 내 모든 트래픽을 감시하고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
카드회원 데이터 환경 내 모든 트래픽을 감시하고 의심되는 침해에 대해 직원에게 경보한다. 모든 IDS 및 IPS 엔진은 최신의 상태로 유지한다.	**11.4.b** 의심되는 침해에 대해 직원에게 직접 경보하도록 IDS / IPS 가 구성되었는지 확인한다.			
	11.4.c IDS/IPS 설정을 검사하여 최적의 보호 기능을 유지하기 위하여 IDS/IPS 장비가 벤더의 지시사항에 딸 설정/유지/갱신되고 있는지 확인한다.			
11.5 파일 무결성 감시 소프트웨어를 사용하여 중요 시스템 파일, 환경 설정 파일 또는 내용 파일의 비인가된 변경을 직원에게 경보하고, 중요 파일의 비교 작업을 적어도 매주 수행하도록 소프트웨어를 설정한다. *주: 파일 무결성 감시 목적으로 중요 파일이란 정기적으로 변경되는 파일은 아니지만 변경이 있을 경우 시스템 침해기 있거나 침해의 위험이 있다는 것을 보여주는 파일이다. 파일 무결성 감시 제품은 일반적으로 OS 관련 파일을 대상으로 기본 설정이 되어 있다. 자체 개발한 어플리케이션과 같은 기타 중요 파일은 사업체--즉, 해당 가맹점이나 서비스 프로바이더--에 의해 평가되고 정의되어야 한다.*	**11.5** 시스템 셋팅, 감시되는 파일을 관찰하고 감시 활동의 결과물을 검토하여 카드회원데이터 환경 안에서 파일 무결성 감시 제품이 사용되고 있는지를 확인한다. 감시되어야 하는 파일의 예: ▪ 시스템 실행 파일 ▪ 응용 프로그램 실행 파일 ▪ 설정 및 변수 파일 ▪ 중앙으로 저장되는--히스토리 또는 아카이브--로그 및 감사 파일			

정보보호 정책 유지관리

요구사항 12: 직원과 계약자들의 정보보호를 위한 정책을 유지한다.

엄격한 정보보호 정책은 전사적인 정보보호 방향(security tone)을 설정하며, 직원들이 준수해야 할 사항들을 제시한다. 모든 직원들은 데이터의 민감도 및 데이터 보호 책임을 인지하여야 한다. 이 요구사항의 목적과 관련하여 "직원"이란 회사의 사옥에 "상주"하는 정규 및 파트타임 직원, 임시직원과 임시인원, 하도급 인원 및 컨설턴트를 지칭한다.

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.1 다음 사항들이 포함된 정보보호 정책을 수립, 공표, 유지 관리 및 배포한다:	12.1 정보보호 정책을 점검하여, 정보보호 정책이 모든 관련 시스템 사용자(벤더, 계약자 및 사업 파트너 포함)에게 공표 및 배포되고 있는지 확인한다.			
12.1.1 모든 PCI DSS 요구사항을 다루어야 한다.	12.1.1 정책이 모든 PCI DSS 요구사항을 다루고 있는지 확인한다.			
12.1.2 위협과 취약점을 파악하고 공식적인 위험 평가를 수행하는 연간 프로세스가 포함되어야 한다.	12.1.2 정보보호 정책에 위협과 취약점을 파악하고 공식적인 위험 평가를 수행하는 연간 프로세스가 포함되어 있는지 확인한다.			
12.1.3 최소 매년 검토하도록 포함하고, 환경이 변화되었을 경우 갱신한다.	12.1.3 정보보호 정책이 최소 매년 검토되어지고, 사업 목표나 위험 환경의 변화를 반영하기 위하여 갱신되어지는지 확인한다.			
12.2 이 문서에 포함된 요구사항에 부합하는 일일 운영 보안 절차를 수립한다. (예: 사용자 계정 관리절차, 로그 검토 절차)	12.2.a 일일 운영 보안 절차들을 점검한다. 절차들이 본 문서 상의 요구사항과 부합하며, 각 요구사항에 대한 관리 및 기술적 절차를 포함하고 있는지 확인한다.			
12.3 직원들이 사용하는 중요한 기술들--예를 들면, 원격 접근 기술, 무선 기술, 이동 전자 매체, 랩탑, PDA, 이메일 사용 및 인터넷 사용--에 대한 사용 정책을 제정하여 모든 직원과 계약업체들이 적절히 사용할 수 있도록 해야 한다. 사용 정책에는 다음 사항들이 포함되어야 한다:	12.3 직원들이 사용하는 중요한 기술들에 대한 사용 정책을 입수/검토하여 다음 내용을 이행하고 있는지 확인한다:			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.3.1 명시적 관리자 승인	12.3.1 사용 정책에서 장비의 사용시 관리자의 명시적 승인을 요구하는지 확인한다.			
12.3.2 기술 사용에 대한 인증	12.3.2 사용 정책에서 모든 기술의 사용시 사용자 ID 와 패스워드 혹은 다른 인증 아이템(예: 토큰)을 사용하여 인증하도록 요구하고 있는지 확인한다.			
12.3.3 해당되는 모든 장비의 목록과 사용자 목록	12.3.3 사용 정책에서 해당 장비의 목록 및 해당 장비 사용을 승인받은 사용자의 목록을 요구하는지 확인한다.			
12.3.4 소유자, 연락처, 사용 목적이 명시된 장비 라벨링	12.3.4 사용 정책에서 장비의 소유자, 연락처, 사용 목적을 포함한 라벨링을 요구하고 있는지 확인한다.			
12.3.5 해당 기술의 합당(acceptable)한 사용	12.3.5 사용 정책에서 해당 기술의 합당(acceptable)한 사용에 대하여 요구하고 있는지 확인한다.			
12.3.6 해당 기술에 대한 네트워크 상의 합당(acceptable)한 위치	12.3.6 사용 정책에서 해당 기술에 대한 네트워크 상의 합당한 이용 위치를 요구하고 있는지 확인			
12.3.7 회사가 승인한 제품 목록	12.3.7 사용 정책에서 회사가 승인한 제품 목록을 요구하고 있는지 확인한다.			
12.3.8 특정 시간 동안 활동이 없을 경우 자동으로 원격 접근 기술에 대한 세션을 종료	12.3.8 사용 정책에서 특정 시간 동안 활동이 없을 경우 자동으로 원격 접근 기술에 대한 세션을 종료하도록 요구하고 있는지 확인한다.			
12.3.9 벤더를 위한 원격 접근 기술의 구동은 필요할 때에만 이루어지며 사용 후 즉시 구동 중지	12.3.9 사용 정책에서 벤더를 위한 원격 접근 기술의 구동은 필요할 때에만 이루어지며 사용 후 즉시 구동 중지하도록 요구하고 있는지 확인한다.			
12.3.10 원격 접근 기술을 통해 원격으로 카드회원 데이터에 접근할 경우 로컬 하드디스크 및 이동 전자 매체에 복사, 이동, 저장하는 것을 금지한다.	12.3.10 사용 정책에서 원격 접근 기술을 통해 원격으로 카드회원 데이터에 접근할 경우 로컬 하드디스크 및 이동 전자 매체에 복사, 이동, 저장하는 것을 금지하고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.4 정보보호 정책과 절차는 모든 직원과 계약업체의 정보보호와 관련한 책임을 명확히 규정해야 한다.	12.4 정보보호 정책이 모든 직원과 계약업체의 정보보호와 관련한 책임을 규정하고 있는지 확인한다.			
12.5 직원 또는 팀에게 다음과 같은 정보보호 관리 책임을 할당한다:	12.5 CSO (Chief Security Officer) 혹은 경영진 중에서 보안과 관련한 임원에게 정보보호와 관련된 임무가 공식적으로 할당되어 있는지 확인한다. 정보보호 정책 및 절차를 통해 다음과 같은 정보보호 관련 책임이 구체적이고 공식적으로 할당되어 있는지 확인한다:			
12.5.1 정보보호 정책과 절차의 수립, 문서화 및 배포한다.	12.5.1 정보보호 정책 및 절차의 수립/배포에 관한 책임이 공식적으로 할당되어 있는지 확인한다.			
12.5.2 보안과 관련된 경고 및 정보를 감시/분석하고 이를 적정한 인력에게 배포한다.	12.5.2 보안과 관련된 경고를 감시 및 분석하고 해당 정보를 적합한 정보보호 부서 및 업무부서 임원에게 배포하는 책임이 공식적으로 할당되어 있는지 확인한다.			
12.5.3 모든 상황을 적시에 그리고 효과적으로 대처하기 위한 보안사고 대응 및 보고 절차를 수립/문서화/배포한다.	12.5.3 보안사고 대응 및 보고 절차의 수립과 배포에 관한 책임이 공식적으로 할당되어 있는지 확인한다.			
12.5.4 추가, 삭제 및 수정을 포함한 사용자 계정을 관리한다.	12.5.4 사용자 계정 관리 및 인증 관리에 대한 책임이 공식적으로 할당되어 있는지 확인한다.			
12.5.5 데이터에 대한 모든 접근을 감시하고 통제한다.	12.5.5 데이터에 대한 모든 접근을 감시하고 통제하는 책임이 공식적으로 할당되어 있는지 확인한다.			
12.6 카드회원 데이터 보호의 중요성을 모든 직원들이 인식할 수 있도록 공식적인 보안 인식 프로그램을 이행한다.	12.6.a 모든 직원들을 대상으로 하는 공식적인 보안 인식 프로그램이 존재하는지 확인한다.			
	12.6.b 보안 인식 프로그램의 절차와 관련 문서를 확보 및 검토하고, 다음 사항을 수행한다:			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.6.1 채용할 때와 최소 연 1 회 직원을 교육한다.	12.6.1.a 보안 인식 프로그램에서 인식 제고와 직원 교육을 위한 다양한 방법을 제공하는지 확인한다. (예, 포스터, 공식문서, 메모, 웹 기반 교육, 회의, 홍보 행사 등)			
	12.6.1.b 모든 직원들이 채용될 때와 최소 연 1 회 정보보호 교육에 참석하는지 확인한다.			
12.6.2 직원들에게 회사의 정보보호 정책 및 절차를 읽었으며, 이해하고 있음을 최소한 연 1 회 인정하도록 요구한다.	12.6.2 보안인식 프로그램은 임직원들이 최소한 연 1 회 회사의 보안정책을 읽었으며, 이해하고 있음을 인정하도록(예를 들어, 서면이나 시스템 상으로) 요구하고 있는지 확인한다.			
12.7 내부로부터의 공격 위험을 최소화하기 위하여 잠재적 직원의 고용 이전에 적격 심사를 수행한다. (9.2 에서 "직원"의 정의 참조) *매장 계산원과 같이 거래 처리를 위해 한 번에 하나의 카드번호만 접근하는 직원의 경우 이 요건은 의무가 아니라 권고사항이다.*	12.7 인사관리 부서에 조회하여 카드회원 데이터나 카드회원 데이터 환경에 접근하게 될 직원들에 대해 고용 이전에 적격 심사--해당 국가의 법 테두리 내에서--가 수행되고 있는지 확인한다. (예를 들어, 경력, 전과 조회, 신용 이력, 신원 조회 등)			
12.8 카드회원 데이터가 서비스 제공업체와 공유된다면, 다음 사항을 포함하여 서비스 제공업체를 관리하기 위한 정책과 절차를 유지하고 이행한다:	12.8 평가 대상 사업체가 서비스 제공업체--예를 들어, 백업 테이프 저장 시설, 웹호스팅 회사나 보안 서비스 제공업체 같은 관리형 서비스 제공업체, 또는 부정 유형 작성을 위하여 데이터를 받는 서비스 제공업체--와 카드회원 데이터를 공유한다면, 관찰, 정책과 절차의 검토, 그리고 지원 문서의 검토를 통해, 다음 사항을 수행한다:			
12.8.1 서비스 제공업체의 목록을 유지한다.	12.8.1 서비스 제공업체의 목록이 유지되고 있는지 확인한다.			
12.8.2 서비스 제공업체가 소유한 카드회원 데이터의 보안에 대해서는 서비스 제공업체가 책임이 있음을 인정한 내용이 포함된 서면 상의 협약을 유지한다.	12.8.2 카드회원 데이터의 보안에 대한 서비스 제공업체의 책임을 서비스 제공업체가 인정하는 서면 상의 협약을 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.8.3 계약에 앞서 적합 실사를 포함하는 서비스 제공업체의 계약을 위한 프로세스를 수립한다.	12.8.3 모든 서비스 제공업체와의 계약 이전의 적합 실사를 포함한 정책 및 절차가 문서화되고 준수되는지 확인한다.			
12.8.4 서비스 제공업체의 PCI DSS 준수 상태를 감시할 수 있는 프로그램을 유지한다.	12.8.4 서비스 제공업체의 PCI DSS 준수 상태를 감시하는 프로그램을 유지하고 있는지 확인한다.			
12.9 침해사고 대응 계획을 수립한다. 시스템 침해사고에 즉시 대처할 수 있도록 준비한다.	12.9 침해사고 대응 계획 혹은 관련 절차를 점검하고, 다음을 수행한다:			
12.9.1 시스템 침해 사고 발생시 적용할 침해사고 대응 계획을 수립한다. 최소한 계획이 다음 사항을 다루어야 한다: ▪ 사고 발생시 최소한 지급결제 브랜드로 통지할 것을 포함하는 역할, 책임 및 커뮤니케이션과 연락 전략 ▪ 구체적인 침해사고 대응 절차 ▪ 사업 복구 및 연속성 절차 ▪ 데이터 백업 프로세스 ▪ 사고의 보고에 대한 법적 요구사항 분석 ▪ 전체 중요 시스템 구성 요소의 범위 및 대응 ▪ 지급결제 브랜드에서 제공받은 침해사고 대응 절차를 참조하거나 포함시킴	12.9.1 침해사고 대응 계획이 다음을 포함하는지 확인한다: ▪ 사고 발생시 최소한 지급결제 브랜드로 통지할 것을 포함하는 역할, 책임 및 커뮤니케이션과 연락 전략 ▪ 구체적인 침해사고 대응 절차 ▪ 사업 복구 및 연속성 절차 ▪ 데이터 백업 프로세스 ▪ 사고의 보고에 대한 법적 요구사항 분석 (예를 들어, 캘리포니아 거주자를 데이터베이스에 보관하는 모든 사업에 대해 침해사고가 실제로 일어나거나 의심되면, 영향을 받는 고객들에게 알릴 것을 요구하는 캘리포니아 법 1386) ▪ 전체 중요 시스템 구성 요소의 범위 및 대응 ▪ 지급결제 브랜드에서 제공받은 침해사고 대응 절차를 참조하거나 포함시킴			
12.9.2 최소 연 1 회 침해사고 대응계획을 시험한다.	12.9.2 침해사고 대응 계획이 최소한 매년 시험되고 있는지 확인한다.			

PCI DSS 요구사항	시험 절차	적용	미적용	목표일 / 비고
12.9.3 침해 경보에 대응하기 위해 일주일, 24 시간 내내 감시 인원을 배정한다.	12.9.3 정보보호 정책의 검토와 관찰을 통하여, 비인가된 활동의 증거, 주요 IDS 경보, 무허가 무선 AP 의 감지 및/혹은 주요 시스템이나 내용 파일에 대한 비인가된 변경에 대한 보고 등에 대비하기 위하여 일주일, 24 시간 내내 사고 대응 및 감시 체계가 구축되어 있는지 확인한다.			
12.9.4 보안 침해사고 대응 책임이 있는 직원에 대한 적절한 교육훈련을 실시한다.	12.9.4 관찰 및 정보보호 정책에 대한 검토를 통하여, 보안 침해사고 책임이 있는 직원들이 정기적으로 교육훈련을 받고 있는지 확인한다.			
12.9.5 침입 탐지, 침입 예방 및 파일 무결성 감시 시스템으로부터의 경보를 포함한다.	12.9.5 관찰과 검토를 통해, 무허가 무선 AP 의 탐지를 포함하는 보안 시스템의 감시 및 경보에 대응하는 프로세스가 침해사고 대응 계획에 포함되어 있는지 확인함			
12.9.6 습득된 경험과 업계의 발전에 따라 침해사고 대응 계획을 수정하고 발전시키는 프로세스를 개발한다.	12.9.6 관찰 및 정책 검토를 통하여, 습득된 경험과 업계의 발전에 따라 침해사고 대응 계획을 수정하고 발전시키는 프로세스가 존재하는지 확인한다.			

부록 A: 공유 호스팅 제공업체를 위한 추가적인 PCI DSS 요구사항

요구사항 A.1: 공유 호스팅 제공업체는 카드회원 데이터 환경을 보호해야 한다.

요건 12.8 에 언급되고 있는 대로, 카드 소유자 데이터에 접근하는 모든 서비스 프로바이더(공유 호스팅 프로바이더를 포함)는 PCI DSS 에 따를 필요가 있습니다. 게다가 요건 2.4 에는, 공유 호스팅 프로바이더는 각 사업체의 호스트 되고 있는 환경 및 데이터를 보호할 필요가 있다고 기재되어 있습니다. 따라서, 공유 호스팅 프로바이더는, 별도로 이 부록에 기재되어 있는 요건을 따를 필요가 있습니다.

요구사항	시험 절차	적용	미적용	목표일/비고
A.1 A.1.1~A.1.4 에 따라서 각 사업체--가맹점, 서비스 제공업체, 또는 기타 사업체--의 호스팅 받는 환경과 데이터를 보호한다. 호스팅 제공업체는 본 요건들과 PCI DSS 의 그 외의 모든 연관 내용들을 만족시켜야 한다. 주: 호스팅 제공업체가 본 요건들을 만족시킬 수 있다고 하더라도, 그 호스팅 제공업체를 이용하는 사업체의 준수가 보장되는 것은 아니다. 각 사업체는 PCI DSS 를 준수해야 하고 해당 여부에 따라 준수 여부를 검증해야 한다.	**A.1** 특별히 공유 호스팅 제공업체에 대한 PCI DSS 평가의 경우, 공유 호스팅 제공업체가 사업체--가맹점과 서비스 제공업체--의 호스팅 받는 환경과 데이터를 보호하고 있는지를 확인하기 위하여, 호스트 받는 가맹점과 서비스 제공업체의 대표 표본으로부터 서버의 표본 (Microsoft Windows 및 Unix/Linux)을 선정하여, 이하 A.1.1 ~ A.1.4 를 수행한다.			
A.1.1 각 사업체가 해당 사업체의 카드회원 데이터 환경에 접근하는 프로세스만을 실행하도록 해야 한다.	**A.1.1** 공유 호스팅 제공업체가 사업체--예를 들어, 가맹점과 서비스 제공업체--로 하여금 사업체의 어플리케이션을 실행하게 하는 경우에, 해당 어플리케이션 프로세스가 사업체의 고유 ID 를 사용하여 실행되는지 확인한다. 예를 들면 아래와 같다: ▪ 시스템 상의 어떠한 사업체도 웹서버 사용자 ID 를 공유하여 사용할 수 없다. ▪ 사업체에 의해 사용되는 모든 CGI 스크립트는 반드시 그 사업체의 고유 사용자 ID 를 사용하여 작성되고 실행되어야 한다.			
A.1.2 각 사업체의 접근 및 권한을 해당 사업체의 카드회원 데이터 환경으로만 제한한다.	**A.1.2.a** 모든 어플리케이션 프로세스의 사용자 ID 가 특권을 가진 사용자 (루트, 관리자 계정)가 아니라는 것을 확인한다.			

요구사항	시험 절차	적용	미적용	목표일/비고
	A.1.2.b 각 사업체--가맹점, 서비스 제공업체--가 해당 사업체가 소유하는 파일 및 디렉토리에 대해서, 혹은 필요한 시스템 파일--파일 시스템 권한, 접근 제어 리스트, chroot, jailshell 등에 의해 제한됨--에 대해서만, 읽기, 쓰기, 혹은 실행 권한을 가지고 있다는 것을 확인한다. 중요: 사업체의 파일을 그룹으로 공유하는 것은 안된다.			
	A.1.2.c 사업체의 사용자가 공유된 시스템 바이너리에 쓰기 접근권한을 가지고 있지 않은 것을 확인한다.			
	A.1.2.d 로그 엔트리를 볼 수 있는 자가 그것을 소유하고 있는 사업체로 제한되어 있는 것을 확인한다.			
	A.1.2.e 각 사업체가 서버의 리소스를 독점하여 취약성--예를 들면, 버퍼 오버플로우 같은 것을 일으킬 수 있는 에러, 경쟁, 재부팅을 일으키는 상황 등--을 악용하지 못하도록 하기 위하여, 아래의 시스템 리소스의 이용에 관하여 제한을 두고 있는지를 확인한다. ▪ 디스크 공간, 대역폭, 메모리, CPU			
A.1.3 로깅 및 감사 기록이 각 사업체의 카드회원 데이터 환경에 맞게 활성화 되어 있고 PCI DSS 요구사항 10 과 일치하도록 한다.	**A.1.3.a** 공유 호스팅 제공업체가, 각 가맹점 및 서비스 제공업체 환경에 대해서, 다음과 같이 로깅을 활성화 하는지 확인한다. ▪ 일반적인 써드파티 어플리케이션의 로그를 적용시키고 있다. ▪ 로그가 액티브한 것이 디폴트로 되어 있다. ▪ 사업체가 로그를 검토할 수 있다. ▪ 사업체에게 로그가 어디에 있는지를 명확하게 알리고 있다.			
A.1.4 호스팅 받고 있는 가맹점 또는 서비스 제공업체에 침해가 발생한 경우, 제시간에 포렌식 조사를 제공하는 프로세스가 가능하다.	**A.1.4** 공유 호스팅 제공업체가, 침해가 발생한 경우에 관련 서버에 제시간에 포렌식 조사를 제공하는 문서화된 정책을 보유하고 있는지 확인한다.			

부록 B: 보완 통제

사업체가 정당한 기술상 또는 문서화 된 비즈니스상의 제약으로 인해 명시적으로 기재된 요구사항을 충족시킬 수 없고, 기타 또는 보완 통제를 통해서, 해당 요구사항에 관련된 위험을 충분히 줄이고 있는 경우, 대부분의 PCI DSS 요구사항에 대해서 보완 통제를 검토할 수 있다.

보완 통제는 이하의 조건을 충족시켜야 한다:

1. 원래의 PCI DSS 요구사항의 의도하는 바를 충족시켜야 하고, 엄격하게 적용되어야 한다.
2. 원래의 PCI DSS 요구사항과 유사한 보호 수준을 제공하여, 원래의 PCI DSS 요구사항이 대응하고자 하는 위험을 보완 통제가 충분히 상쇄시킬 수 있어야 한다. (각 PCI DSS 요구사항의 의도에 대해서는 *Navigating PCI DSS* 을 참조하라.)
3. 다른 PCI DSS 요구사항을 "초과 (above and beyond)" 하여야 한다. (단순히 다른 PCI DSS 요구사항 항목들을 충족시키고 있다는 것만으로는 보완 통제라고 할 수가 없다.)

   보완 통제가 다른 PCI DSS 요구사항을 "초과" 하는지 판단할 때, 다음 사항을 고려한다:

   주: 아래의 항목 a) 부터 c)까지는 단순히 예를 보여주기 위함이다. 모든 보완 통제는 PCI DSS 감사를 수행하는 평가자가 충분성을 검토하고 검증해야 한다. 보완 통제가 유효한지는 해당 통제가 이행되는 환경, 그러한 환경을 둘러싼 보안 통제들, 그리고 해당 보안 통제의 설정이 어떻게 되어 있는지에 따라 좌우된다. 회사는 특정한 보안 통제가 모든 환경에 유효하게 적용되는 것은 아니라는 것을 인지해야 한다.

   a) 기존의 PCI DSS 요구사항들이 검토중인 해당 항목에 이미 요구되는 경우, 해당 요구사항들은 보완 통제로 간주 **할 수 없다**. 예를 들어, 콘솔을 통하지 않은 관리자 접속의 패스워드들은 평문 상태의 관리자 패스워드 도청의 위험을 줄이기 위하여 암호화되어 전송되어야 한다. 사업체는 다른 PCI DSS 패스워드 요구사항들(침입자 잠금, 복잡한 패스워드 사용 등)을 패스워드를 암호화하지 않은 것에 대한 보완 통제 내용으로 사용할 수 없는데, 그 이유는 이러한 다른 패스워드 요구사항들은 평문으로 되어 있는 패스워드 도청의 위험을 줄여주지 않기 때문이다. 또한 이러한 다른 패스워드 통제들은 이미 검토중인 해당 항목에 대한 PCI DSS 요구사항들이다.

   b) 기존의 PCI DSS 요구사항들이 다른 영역에서 요구되고 있지만, 원래 검토중인 해당 항목에서는 요구되어 있지 않은 경우, 해당 요구사항들은 보완 통제로 간주 **할 수 있다**. 예를 들어, 2 팩터 인증은 원격 접속에 대한 PCI DSS 요구사항이다. 콘솔을 통하지 않은 관리자 접속에서 암호화된 패스워드의 전송이 지원되지 않을 때 내부 네트워크에서의 2 팩터 인증을 보완 통제로 고려할 수 있다. 2 팩터 인증이 다음 조건을 만족시킨다면 적절한 보완 통제가 될 수 있다: (1) 해당 보완 통제가 평문 상태의 관리자 패스워드 도청의 위험을 다룸으로써 원래 요구사항의 의도를 충족시키고, (2) 해당 보완 통제가 적절히 설정되고 안전한 환경을 유지한다.

   c) 기존의 PCI DSS 요구사항들이 새로운 통제와 조합되어 보완 통제가 될 수 있다. 예를 들어, 기업이 요구사항 3.4 에 따라서 (암호화 등에 의해서) 카드소유자 데이터를 읽을 수 없게 하는 것이 불가능한 경우, 보안 통제는 다음 사항 모두를 다루는 디바이스 장치 혹은 디바이스 장치, 어플리케이션, 통제의 조합으로 구성될 수 있다: (1) 내부 네트워크 분리, (2) IP 주소 또는 MAC 주소 필터링, (3) 내부 네트워크로부터의 2 팩터 인증.
4. 해당 PCI DSS 요구사항에 따르지 않음으로써 생길 수 있는 추가적인 위험을 고려해야 한다.

평가자는, 위의 1-4 항목에 따라서, 매년 PCI DSS 평가에서 보완 통제를 철저하게 평가하여 각각의 보완 통제가 원래의 PCI DSS 요구사항이 다루도록 설계된 위험을 적절하게 다루고 있는지 검증해야 한다. 준수 상태를 유지하기 위하여, 평가가 완료된 이후에 보완 통제가 효과를 유지하도록 하는 프로세스와 통제가 적용되어야 한다.

부록 C: 보완 통제 워크시트

이 워크시트를 사용하여 PCI DSS 요구사항을 만족하기 위해 보완 통제가 사용되고 있는 모든 요구사항들에 대해 보완 통제를 정의한다. 보완 통제는 표준 준수 보고서 안의 이와 대응하는 PCI DSS 요구사항 섹션 안에도 문서화시킬 필요가 있음에 유의한다.

주: *위험 분석을 실시하고, 합당한 기술적 또는 문서화된 비즈니스상의 제약을 가지고 있는 회사들만이 준수를 위해 보완 통제의 사용을 고려할 수 있다.*

요구사항 번호 및 정의:

	필요한 정보	설명
1. **제약사항**	원래 요구사항의 준수를 저해하는 제약사항을 나열한다.	
2. **목적**	원래 통제의 목적을 정의하고, 보완 통제에 의해 충족될 수 있는 목적을 정의한다.	
3. **식별된 위험**	원래 통제의 결여로 인해 발생하는 모든 추가적인 위험을 식별한다.	
4. **보완 통제의 정의**	보완 통제를 정의하고, 보완 통제가 원래 통제의 목적 및 (있다면) 증가된 위험을 어떻게 다루고 있는지 설명한다.	
5. **보완 통제의 검증**	보완 통제를 어떻게 검증하고 시험할 것인지 정의한다.	
6. **유지관리**	보완 통제를 유지하기 위해 적용된 프로세스와 통제사항을 정의한다.	

보완통제 워크시트 – 완성 예제

요구사항에 "적용"으로 표시되어 있고 "목표일/비고" 열에 보완 통제가 언급되어 있는 모든 요구사항에 대해서 본 워크시트를 사용하여 보완 통제를 정의한다.

□□□□ □□: ***8.1—*** *모든 사용자에게 고유 ID 를 할당한 후에 시스템 구성요소 혹은 카드회원 데이터에 대한 접근을 허용하여야 한다.*

	필요한 정보	설명
1. **제약사항**	원래 요구사항의 준수를 저해하는 제약사항을 나열한다.	*XYZ 회사는 독립된 유닉스 서버들을 LDAP 없이 사용하고 있다. 따라서, 서버들 각각은 "root" 로그인을 필요로 한다. XYZ 회사가 "root" 로그인을 관리하는 것도 불가능하고, 각각의 사용자 별로 모든 "root" 활동을 로그로 기록하는 것도 가능하지 않다.*
2. **목적**	원래 통제의 목적을 정의하고, 보완 통제에 의해 충족될 수 있는 목적을 정의한다.	*고유한 로그인을 필요로 하는 목적은 두 가지이다. 첫번째로, 로그인 자격을 공유하는 것은 보안 관점으로 볼 때 바람직하다고 보여지지 않는다. 둘째로, 로그인을 공유하게 되면 어떤 개인이 특정한 행동에 대해 책임이 있다고 명확하게 말할 수 없게 된다.*
3. **식별된 위험**	원래 통제의 결여로 인해 발생하는 모든 추가적인 위험을 식별한다.	*모든 개인이 고유 ID 를 가지고 있고 추적될 수 있다는 것을 보증하지 못하게 됨으로써 접근 통제 시스템에 추가적인 위험이 발생한다.*
4. **보완 통제의 정의**	보완 통제를 정의하고, 보완 통제가 원래 통제의 목적 및 (있다면) 증가된 위험을 어떻게 다루고 있는지 설명한다.	*XYZ 회사는 SU 명령어를 사용하여 그들의 데스크탑에서 서버로 로그인 하도록 종업원에게 요구하려고 한다. SU 명령어는 사용자가 "root" 계정으로 접근하여 "root" 계정 하에서 작업하는 것을 허락한다. 하지만 SU-log 디렉터리에 로그를 남길 수 있다. 이러한 방법을 통하여 각각의 사용자의 행동은 SU 명령어를 통해 추적될 수 있다.*
5. **보완 통제의 검증**	보완 통제를 어떻게 검증하고 시험할 것인지 정의한다.	*XYZ 회사는 평가자에게 SU 명령이 실행되고 있고, 이 명령어를 사용하는 개인들은 로그에 기록되어 해당 개인이 루트 권한 하에서 수행하는 내역을 식별할 수 있음을 시연해 보인다.*
6. **유지관리**	보완 통제를 유지하기 위해 적용된 프로세스와 통제사항을 정의한다.	*XYZ 회사는 개별 사용자가 개별적으로 추적 혹은 로그 기록이 없이 root 명령들을 실행 가능하도록 SU 설정사항을 변경, 수정 또는 제거하지 못하도록 하는 프로세스와 절차를 문서화 한다.*

부록 D: 준수 증명서 – 가맹점

Payment Card Industry (PCI)
데이터 보안 표준

현장 평가의 준수 증명서 – 가맹점

버전 1.2

2008 년 10 월

작성 지침

본 문서는 PCI DSS 에 대한 가맹점의 준수 상태 신고서로 QSA 혹은 (가맹점 내부 감사부서에서 검증을 수행하였을 경우에) 가맹점이 작성해야 한다. 모든 해당 부분을 작성한 후에 매입사 또는 요구하는 지급결제 브랜드에 제출한다.

파트 1. Qualified Security Assessor 회사 정보					
회사 명:					
선임 QSA 이름:			직위:		
전화:			E-mail:		
회사 주소:			시:		
도:		국가:		ZIP:	
URL:					

파트 2. 가맹점 조직 정보					
회사 명:			DBA(s):		
담당자 이름:			직위:		
전화:			E-mail:		
회사 주소:			시:		
도:		국가:		ZIP:	
URL:					

파트 2a. 가맹점 업무의 유형 (해당사항 모두 표시)

☐ 소매 ☐ 정보통신 ☐ 식료잡화 및 슈퍼마켓

☐ 석유 ☐ 전자상거래 ☐ 통신판매

☐ 관광 및 엔터테인먼트 ☐ 기타 (구체적으로 기재):

PCI DSS 검토에 포함된 설비 및 장소 목록 기재:

파트 2b. 관계

귀사는 한 개 이상의 제 3 자 업체와 관계를 가지고 있는가(예를 들면, 게이터웨이, 웹 호스팅 업체, 항공 예약 에이전트, 로열티 프로그램 에이전트 등)? ☐ 예 ☐ 아니오

귀사는 두 개 이상의 매입사와 관계를 가지고 있는가? ☐ 예 ☐ 아니오

파트 2c. 거래 처리

사용중인 지급결제 어플리케이션: 지급결제 어플리케이션 버전:

파트 3. PCI DSS 검증

(ROC의 날짜) 시점의 표준 준수 보고서("ROC")*에 기록된 결과에 기초하여, (QSA 이름/가맹점 이름)* 는 *(날짜)* 현재 본 문서의 파트 2에 식별된 사업체에 대해 다음과 같이 준수 상태를 선언한다(택일):

☐ **준수:** ROC 내의 모든 요구사항들이 "적용[4]"으로 표시되었고, PCI SSC ASV *(ASV 이름)*에 의해 스캔이 통과되어 *(가맹점 회사 명)*은 PCI DSS *(버전 번호 입력)*을 온전히 준수하고 있음을 입증하였다.

☐ **미준수:** ROC 내의 일부 요구사항들이 "미적용"으로 표시되어 전반적으로 **미준수**로 결과가 나왔거나, PCI SSC ASV 에 의해 스캔이 통과되지 않아, *(가맹점 회사 명)* 은 PCI DSS 를 온전히 준수하고 있음을 입증하지 못하였다.

준수를 위한 **목표 일**:

미준수 상태로 본 서식을 제출하는 사업체는 본 문서의 파트 4에 있는 실행 계획을 작성할 필요가 있을 수 있다. *파트 4를 작성하기 전에 귀사의 매입사나 지급결제 브랜드에 문의해야 한다.*

파트 3a. 준수 상태의 확인

QSA/가맹점은 다음과 같이 확인한다:

☐	ROC는 *PCI DSS 요구사항 및 보안 평가 절차*, 버전*(버전 번호 입력)*에 따라 작성되었으며, 해당 문서의 지침에 따라 작성되었다.
☐	상기한 ROC와 본 증명서 내의 모든 정보는 평가 결과를 모든 측면에서 공정하게 반영하고 있다.
☐	가맹점은 지급결제 어플리케이션이 승인 이후에 민감한 인증 정보를 저장하지 않는다는 사실을 지급결제 어플리케이션 벤더와 확인하였다.
☐	가맹점은 PCI DSS를 읽었으며 가맹점은 항상 PCI DSS를 온전히 준수해야 한다는 것을 인정한다.
☐	평가 중에 모든 시스템에서 승인 이후에 마그네틱 선 (즉, 트랙) 데이터[5], CAV2, CVC2, CID, CVV2 데이터[6], PIN 데이터[7] 저장의 증거가 발견되지 않았다.

파트 3b. QSA 및 가맹점 확인

선임 QSA의 서명 ↑	***날짜:***
선임 QSA 이름:	***직위:***

가맹점 임원의 서명 ↑	***날짜:***
가맹점 임원 이름:	***직위:***

[4] "적용" 결과들에는 QSA/가맹점 내부 감사인이 검토한 보완 통제를 포함해야 한다. 보완 통제들이 해당 요구사항과 관련된 위험을 충분히 감소시킬 수 있는 것으로 판단한다면, QSA는 해당 요구사항을 "적용"으로 표시해야 한다.

[5] 대면 거래에서 승인을 위해 사용되는 마그네틱 선에 입력된 데이터. 거래 승인 이후에 전체 마그네틱 선 데이터를 사업체들은 보관하면 아니 된다. 보관할 수 있는 트랙 데이터의 유일한 항목들은 카드 번호, 유효기간, 이름이다.

[6] 비대면 거래를 확인하기 위해 사용되는, 지블결제 카드의 서명난이나 전면에 인쇄된, 세 자리 또는 네 자리의 숫자.

[7] 대면 거래에서 카드회원이 입력한 개인 식별 번호, 그리고/또는 거래 메시지에 존재하는 암호화된 PIN 블록.

파트 4. 미준수 상태에 대한 실행 계획

각 요구사항에 대해서 적절한 "준수 상태"를 선택하세요. 요구사항에 대해서 귀하가 "아니오"라고 답하였다면, 귀사가 해당 요구사항을 준수하게 될 일정과 해당 요구사항을 충족하기 위해 수행할 조치 사항에 대한 간략한 설명을 기술해야 한다. *모든 지급결제 브랜드가 이 섹션을 요구하는 것은 아니기 때문에 파트 4를 작성하기 전에 귀사의 매입사나 지급결제 브랜드에 문의해야 한다.*

PCI 요구사항	설명	준수 상태 (택일)	조치 일정과 조치 사항 (준수 상태가 "아니오"일 경우)
1	카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다.	☐ 예 ☐ 아니오	
2	시스템 패스워드 및 기타 보안 파라미터에 벤더가 제공한 디폴트 값을 사용하지 않는다.	☐ 예 ☐ 아니오	
3	저장된 카드회원 데이터를 보호한다.	☐ 예 ☐ 아니오	
4	공중망을 통한 카드회원 데이터 전송을 암호화한다.	☐ 예 ☐ 아니오	
5	안티바이러스 소프트웨어를 사용하고 정기적으로 갱신한다.	☐ 예 ☐ 아니오	
6	안전한 시스템과 어플리케이션을 개발하고 유지한다.	☐ 예 ☐ 아니오	
7	업무상 알 필요가 있는지에 따라 카드회원 데이터에 대한 접근을 제한한다.	☐ 예 ☐ 아니오	
8	컴퓨터에 접근하는 사용자별로 고유 ID 를 부여한다.	☐ 예 ☐ 아니오	
9	카드회원 데이터에 대한 물리적 접근을 제한한다.	☐ 예 ☐ 아니오	
10	네트워크 자원과 카드회원 데이터에 대한 모든 접근을 추적하고 감시한다.	☐ 예 ☐ 아니오	
11	보안시스템 및 프로세스를 정기적으로 시험한다.	☐ 예 ☐ 아니오	
12	직원과 계약자들의 정보보호를 위한 정책을 유지한다.	☐ 예 ☐ 아니오	

부록 **E:** 준수 증명서 – 서비스 제공업체

Payment Card Industry (PCI)
데이터 보안 표준

현장 평가의 준수 증명서 – 서비스 제공업체

버전 1.2

2008 년 10 월

작성 지침

본 문서는 PCI DSS 에 대한 서비스 제공업체의 준수 상태 신고서로 QSA 및 서비스 제공업체가 작성해야 한다. 모든 해당 부분을 작성한 후에 요구하는 지급결제 브랜드에 제출한다.

파트 1. Qualified Security Assessor 회사 정보					
회사 명:					
선임 QSA 이름:			직위:		
전화:			E-mail:		
회사 주소:			시:		
도:		국가:		ZIP:	
URL:					

파트 2. 서비스 제공업체 조직 정보					
회사 명:			DBA(s):		
담당자 이름:			직위:		
전화:			E-mail:		
회사 주소:			시:		
도:		국가:		ZIP:	
URL:					

파트 2a. 제공하는 서비스들 (해당사항 모두 표시)

☐ 승인	☐ 로열티 프로그램	☐ 3-D Secure 접근 통제 서버
☐ 스위칭	☐ IPSP (E-commerce)	☐ 마그네틱 선 거래 처리
☐ 페이먼트 게이트웨이	☐ Clearing & Settlement	☐ 통신판매 거래 처리
☐ 호스팅	☐ 발급 처리	☐ 기타 (구체적으로 기재):

PCI DSS 검토에 포함된 설비 및 장소 목록 기재:

파트 2b. 관계

귀사는 한 개 이상의 제 3 자 업체와 관계를 가지고 있는가(예를 들면, 게이터웨이, 웹 호스팅 업체, 항공 예약 에이전트, 로열티 프로그램 에이전트 등)? ☐ 예 ☐ 아니오

파트 2c. 거래 처리

귀사가 카드회원 데이터를 저장, 처리, 전송하는 방법과 용량은?

사용중인 지급결제 어플리케이션: *지급결제 어플리케이션 버전:*

파트 3. PCI DSS 검증

(ROC의 날짜) 시점의 표준 준수 보고서("ROC")*에 기록된 결과에 기초하여, (QSA 이름/가맹점 이름)* 는 *(날짜)* 현재 본 문서의 파트 2에 식별된 사업체에 대해 다음과 같이 준수 상태를 선언한다(택일):

☐ **준수:** ROC 내의 모든 요구사항들이 "적용[8]"으로 표시되었고, PCI SSC ASV *(ASV 이름)*에 의해 스캔이 통과되어 *(서비스 제공업체 명)*은 PCI DSS *(버전 번호 입력)*을 온전히 준수하고 있음을 입증하였다.

☐ **미준수:** ROC 내의 일부 요구사항들이 "미적용"으로 표시되어 전반적으로 **미준수**로 결과가 나왔거나, PCI SSC ASV 에 의해 스캔이 통과되지 않아, *(서비스 제공업체 명)* 은 PCI DSS 를 온전히 준수하고 있음을 입증하지 못하였다.

준수를 위한 **목표 일**:

미준수 상태로 본 서식을 제출하는 사업체는 본 문서의 파트 4에 있는 실행 계획을 작성할 필요가 있을 수 있다. *파트 4를 작성하기 전에 귀사의 매입사나 지급결제 브랜드에 문의해야 한다.*

파트 3a. 준수 상태의 확인

QSA와 서비스 제공업체는 다음과 같이 확인한다:

☐	ROC는 *PCI DSS 요구사항 및 보안 평가 절차*, 버전*(버전 번호 입력)*에 따라 작성되었으며, 해당 문서의 지침에 따라 작성되었다.
☐	상기한 ROC와 본 증명서 내의 모든 정보는 평가 결과를 모든 측면에서 공정하게 반영하고 있다.
☐	가맹점은 PCI DSS를 읽었으며 가맹점은 항상 PCI DSS를 온전히 준수해야 한다는 것을 인정한다.
☐	평가 중에 모든 시스템에서 승인 이후에 마그네틱 선 (즉, 트랙) 데이터[9], CAV2, CVC2, CID, CVV2 데이터[10], PIN 데이터[11] 저장의 증거가 발견되지 않았다.

파트 3b. QSA 및 서비스 제공업체 확인

선임 QSA의 서명 ↑	*날짜:*
선임 QSA 이름:	*직위:*

서비스 제공업체 임원의 서명 ↑	*날짜:*
서비스 제공업체 임원 이름:	*직위:*

[8] "적용" 결과들에는 QSA/가맹점 내부 감사인이 검토한 보완 통제를 포함해야 한다. 보완 통제들이 해당 요구사항과 관련된 위험을 충분히 감소시킬 수 있는 것으로 판단한다면, QSA는 해당 요구사항을 "적용"으로 표시해야 한다.

[9] 대면 거래에서 승인을 위해 사용되는 마그네틱 선에 입력된 데이터. 거래 승인 이후에 전체 마그네틱 선 데이터를 사업체들은 보관하면 아니 된다. 보관할 수 있는 트랙 데이터의 유일한 항목들은 카드 번호, 유효기간, 이름이다.

[10] 비대면 거래를 확인하기 위해 사용되는, 지블결제 카드의 서명난이나 전면에 인쇄된, 세 자리 또는 네 자리의 숫자.

[11] 대면 거래에서 카드회원이 입력한 개인 식별 번호, 그리고/또는 거래 메시지에 존재하는 암호화된 PIN 블록.

파트 4. 미준수 상태에 대한 실행 계획

각 요구사항에 대해서 적절한 "준수 상태"를 선택하세요. 요구사항에 대해서 귀하가 "아니오"라고 답하였다면, 귀사가 해당 요구사항을 준수하게 될 일정과 해당 요구사항을 충족하기 위해 수행할 조치 사항에 대한 간략한 설명을 기술해야 한다. *모든 지급결제 브랜드가 이 섹션을 요구하는 것은 아니기 때문에 파트 4를 작성하기 전에 귀사의 매입사나 지급결제 브랜드에 문의해야 한다.*

PCI 요구사항	설명	준수 상태 (택일)	조치 일정과 조치 사항 (준수 상태가 "아니오"일 경우)
1	카드회원 데이터를 보호하기 위해 방화벽 설정을 설치하고 유지한다.	☐ 예 ☐ 아니오	
2	시스템 패스워드 및 기타 보안 파라미터에 벤더가 제공한 디폴트 값을 사용하지 않는다.	☐ 예 ☐ 아니오	
3	저장된 카드회원 데이터를 보호한다.	☐ 예 ☐ 아니오	
4	공중망을 통한 카드회원 데이터 전송을 암호화한다.	☐ 예 ☐ 아니오	
5	안티바이러스 소프트웨어를 사용하고 정기적으로 갱신한다.	☐ 예 ☐ 아니오	
6	안전한 시스템과 어플리케이션을 개발하고 유지한다.	☐ 예 ☐ 아니오	
7	업무상 알 필요가 있는지에 따라 카드회원 데이터에 대한 접근을 제한한다.	☐ 예 ☐ 아니오	
8	컴퓨터에 접근하는 사용자별로 고유 ID 를 부여한다.	☐ 예 ☐ 아니오	
9	카드회원 데이터에 대한 물리적 접근을 제한한다.	☐ 예 ☐ 아니오	
10	네트워크 자원과 카드회원 데이터에 대한 모든 접근을 추적하고 감시한다.	☐ 예 ☐ 아니오	
11	보안시스템 및 프로세스를 정기적으로 시험한다.	☐ 예 ☐ 아니오	
12	직원과 계약자들의 정보보호를 위한 정책을 유지한다.	☐ 예 ☐ 아니오	

부록 F: PCI DSS 검토 — 범위 정의 및 표본의 선택