Security Policy of PCI DSS V3

Since 01/01/15

Overview
This policy is intended to relay the importance of security and protecting cardholder data.

Purpose

• To establish this policy for the secure handling of sensitive card holder data including but not limited to magnetic strip data, Primary Account Numbers (PAN's), expiration date, and service code

Policies to Protect and Manage Cardholder Data

The importance of protecting cardholder data is paramount. Allowing data theft or destruction, inadvertently sharing confidential information, infecting system networks with viruses, misuse of company resources, allowing the theft of company property, and allowing the compromise of private or confidential company or client information are all very real examples of what might result from a security compromise.

1. All sending of unencrypted Primary Account Numbers by end-user messaging technologies (i.e., email, instant messaging, and chat) are strictly prohibited. If a PAN must be sent by end-user messaging, only email is allowed and the PAN will be encrypted using WinZip. The WinZip password will be communicated to the end user by means other than end user messaging (phone or fax is allowed).

2. Access to system components and cardholder data is limited to only those authorized individuals whose job require such access or have a need-to-know. This authority is granted by senior management and reviewed annually.

3. All paper that contains cardholder data is to be identified and physically secured in a locked drawer. No electronic cardholder data will ever be stored.

4. Strict control is to be maintained over the internal or external distribution of any kind of media that contains cardholder data

• Media is classified and clearly marked as confidential

• Media is sent by secured courier or other delivery method that can be accurately tracked

5. Management approval is to be obtained prior to moving any and all media containing cardholder data from a secured area.

6. Strict control must be maintained over the storage and accessibility of media that contains cardholder data.

7. Media containing cardholder data is to be destroyed when it is no longer needed for business or legal reasons.

• Paper materials are to be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.

• The general rule is that media containing cardholder date will be destroyed when over 180 days old. Exceptions to the rule must be approved by senior management.

8. Strong cryptography and security protocols, such as SSL, TLS or IPSEC, are to be used to safeguard sensitive cardholder data during transmission over open, public networks. (This statement is only applicable to those who handle cardholder data via a computer)

Policy Maintenance and Employee/Contractor Awareness

1. Review of this policy will be conducted on an annual basis or as changes to the environment occur

2. Usage of employee-facing technologies such as remote access, wireless, electronic media, internet, PDA's and wireless will adhere to the following:

• No unauthorized equipment can be brought in or set up in this facility. This includes, but is not limited to modems, computers, or wireless devices.

• Wireless devices must be set up securely by establishing secure accounts/passwords, disabling SSID broadcasts, and using the highest available encryption for the device.

3. One or more employees will be designated with security responsibility.

4. Incident response documents will be created, reviewed by all employees, and will be updated on an annual basis.

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

5. These security policies will be formally reviewed annually with all employees/contractors.

6. A list of Service Providers must be maintained. This list will be updated and reviewed by senior management when necessary but at every 180 days.
Visa Fraud Control Group: 1-(650)-432-2978
MasterCard: 1-(636)-722-4100
Discover Card: 1-(800)-347-3083

7. A written Agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service provider possess is required from each Service Provider.

8. Due diligence is to be performed prior to the engagement of Service Providers. Procedures performed will include when possible:

• A visit to the Service Providers physical offices to discuss security practices and procedure with their management and staff.

• A written statement acknowledging their responsibilities to securely process, handle and transmit cardholder data.

• Written proof that the Service Provider is PCI compliant.

• Request reliable industry references.

9. A program is to be maintained to monitor Service Providers' PCI DSS compliance status. On an annual basis a request for a new compliance certificate will be requested.

This policy applies to all employees and systems of

DBA: _____

Security Policy of PCI DSS V3

Since 01/01/15

개요

이 보안 정책은 고객의 크레딧카드 정보를 보호하기 위해 보안의 중요성을 강조하고자 제정되었습니다.

목적

이 보안정책은 Magnetic strip data, Primary Account Numbers (PAN's), expiration date 및 service code 등의 고객의 크레딧 카드 데이터를 안전하게 다루기 위한 정책으로 제정되었습니다.

고객의 크레딧카드 정보에 대한 보호방법

고객의 크레딧카드 정보를 보호하는 것은 매우 중요합니다.
데이터의 도난,파괴 및 부적절한 방법으로 중요 데이터의 공유를 허락하는 것, 시스템 네트워크에 바이러스가 감염되도록 방치하는 것, 회사 정보의 오/남용 및 회사 자원의 도난을 방조하는 것, 회사나 고객의 사적이거나 중요한 정보의 유출을 허용하는 것은 모두 실제 보안사고로부터 발생할 수 있는 사항들입니다.

1. 이메일, 인스턴트 메시지, 채팅등으로 비암호화된 PAN(Primary Account Numbers) 을 전송하는 것은 강력하게 금지되어 있습니다. 만약에 PAN 이 반드시 메시지로 전송이 되어야 한다면, 단지 이메일을 이용한 방법만이 허용되며, 이때에 WinZip 을 사용해서 PAN 이 암호화가 되어야 합니다. WinZip Password 는 메시징 서비스 이외의 전화나 Fax 등으로 전달될 수 있습니다.

2. 카드 정보 및 시스템에 대한 접근은 업무상 꼭 필요한 사람에게만 허용됩니다. 이 허용은 경영자가 알고 있어야 하며 매년 리뷰가 되어야 합니다.

3. 카드 정보가 기록된 매체는 안전한 잠금장치가 있는 장소에 보관되어야 합니다. 이 정보는 전자매체에 저장이 되면 안됩니다.

4. 만약 카드 정보가 기록된 매체가 대내외적으로 다른 곳에 보내질 경우 안전한 전달 방법을 사용하여야 합니다.
- 카드 정보가 기록된 매체는 비밀로 분류되어 취급되어야 합니다.
- 카드 정보가 기록된 매체는 추적가능한 방법으로 전달되어야 합니다.

5. 카드 정보가 기록된 매체가 안전한 장소에서 다른 곳으로 이동할 때에는 사전에 정보 관리자의 승인을 받아야 합니다.

6. 카드 정보에 대한 접근은 업무상 꼭 필요한 사람에게만 허용되어야 합니다.

7. 카드 정보가 기록된 매체가 사업상 또는 법적으로 더 이상 필요가 없어지게 되면 반드시 폐기해야 합니다.
- 폐기할 때 인쇄된 종이는 갈아 버리거나 태워서 재로 만들던지 물에 풀어서 더 이상 카드 정보가 재생되지 못하도록 하여야 합니다.
- 경영자의 판단에 따라 차이가 있을 수 있으나 고객님의 Chargeback 등을 위해서 최소 2 년은 보관하시기 바랍니다.

8. 강력한 암호화 및 안전한 프로토콜 - SSL, TLS 또는 IPSEC – 이 고객의 중요한 카드정보 데이터를 보호되지않은 네트워크 공간에서 전달되고자 할때 반드시 사용되어야 합니다. (이 조항은 컴퓨터를 사용해서 크레딧 카드 정보를 취급하는 사업자에게만 해당됩니다.)

정책 유지 및 직원/서비스 제공자 보안 인식

1. 이 정책은 매년 정기적으로 혹은 환경이 바뀔 때마다 리뷰가 되어야 합니다.

2. 모든 직원과 서비스 제공자가 저장 및 통신 기술 (예. Remote-access 기술, wireless 기술, 휴대용 저장 장치, laptop 컴퓨터, PDA, 이메일, 인터넷 사용)을 사용할 때에는 다음과 같은 사항을 지켜야 합니다.
- 고객의 비지니스 공간에 허가되지 않은 모뎀,컴퓨터, 무선기기등이 비치되거나 설치되서는 안됩니다.
- 무선기기는 안전한 계정/비밀번호, SSID 브로드캐스트의 사용금지 및 가능한 최고수준의 보안기술을 사용하여 설치되어야만 합니다.

3. 한 명 이상의 직원이 보안책임자로 지정되어야 합니다.

4. 사고 대응에 대한 자료는 매년 모든 직원들에 의해서 제정되고 리뷰 및 업데이트가 되어야 합니다. 보안 사고에 대한 대응은 사고 정의, 심각도 분석, 차단, 제거, 복구 및 보안 통제 향상을 위한 원인 결과 분석의 절차를 따를 수 있습니다.

5. 이런 보안정책은 모든 직원과 계약자에 의해서 매년 정식적으로 리뷰가 되어야 합니다.

6. 서비스 제공자의 목록이 관리되어야 합니다. 이 목록은 필요한 경우 매 180 일마다 경영자에 의해서 리뷰 및 업데이트가 되어야 합니다.
Visa Fraud Control Group: 1-(650)-432-2978
MasterCard: 1-(636)-722-4100
Discover Card: 1-(800)-347-3083

7. 서비스 제공자는 서면 계약을 통하여 자신들이 보관하는 카드 정보에 대해서 보안 책임을 진다는 것에 동의하여야 합니다.

8. 서비스 제공자와 계약을 할때에는 상당한 주의가 요구됩니다. 가능한 다음 절차를 따르시기 바랍니다.
- 서비스 제공자의 사무실에 방문해서 보안 정책 및 절차에 대한 상의가 이루어져야 합니다.
- 고객의 크레딧카드 정보를 안전하게 처리, 취급 및 전달하겠다는 서면 계약서가 있어야 합니다.
- 서비스 제공자가 PCI 보안인증을 받았다는 서면 증거가 있어야 합니다.
- 업계에 믿을만한 참고인이 있는지 요청해보아야 합니다.

9. 카드 정보를 공유하는 서비스 제공자는 반드시 PCI DSS 규정을 준수하여야 합니다. 이러한 사항은 업체 선정 이전에 조사하여야 하며 매년 SAQ 인증받을 때 확인하여야 합니다.

이 정책은 모든 직원과 모든 시스템에 적용됩니다.