

Cardholder Information Security Program

Version 5.5



The specific requirements described in the Cardholder Information Security Program constitute minimum required measures for protecting cardholder data. Meeting these minimum requirements alone may not be sufficient to ensure that service providers and merchants comply with the full *Visa U.S.A. Operating Regulations* on this subject. In addition, as technology, market, and regulatory conditions evolve, new measures may become necessary to meet the challenge of providing acceptable levels of protection for cardholder information.

The information furnished herein is proprietary to Visa. It is provided solely for use by Visa Members, Mail Order/Telephone Order (MO/TO) and Internet Merchants, and associated service providers in support of Visa card services programs.

© Copyright 2000 Visa U.S.A.

Version 5.5



Table of Contents

Table of Contents	I
Introduction	1
Who Should Read This Document?	2
Executives	2
Managers	2
Technical Staff	2
Cardholder Information Security Program Overview	3
What Needs to be Protected	3
Key Roles and Responsibilities	4
Visa	4
Role	4
Responsibility	4
Acquirers	4
Role	4
Responsibility	4
Service Providers and Merchants	5
Role	5
Responsibility	5
Program Timeline	5
Compliance and Monitoring	5
Why comply?	6
Part 1: Executive Summary	7
Program Requirements	7
Part 2: Requirements	9
Introduction	9
Logical Data Security	9
Administrative Data Security	15

Physical Data Security.....	17
Appendix A: Firewall Complexes.....	23
Firewall Definition.....	23
Firewall Types.....	24
Packet Filter.....	24
Proxy	26
Hybrid	26
Firewall Standards.....	26
Appendix B: Cryptographic and Key Management Mechanisms	27
Cryptographic System Criteria	27
Key Management Controls.....	29
Access to Keys.....	29
Random Key Generation.....	30
Allowable Key Forms.....	30
Dual Control	31
Split Knowledge	31
Audit Trails.....	31
Intended Key Usage	32
Key Compromise.....	32
Compartmentalization of Risk	32
Cryptographic Strength.....	32
Data Security Vendors	35
Glossary of Terms.....	37
Index.....	41



More and more consumers and businesses are ordering goods and services by mail, over the telephone, and through the Internet. It's fast and easy...but is it safe? That's typically the big question on the minds of most customers.

Introduction

With the explosive growth of “e-tailers” and card-not-present transactions, information security is becoming more important than ever. Consumers who offer their card numbers online, over the phone, or through the mail want assurance that their account information is safe.

That's what the *Visa U.S.A. Cardholder Information Security Program* is all about. As the name implies, its primary purpose is to help establish security procedures to protect cardholder information.

This booklet is the first of a future series that will provide requirements and best practices for securing cardholder information across the various acceptance channels. This particular document, for the card-not-present environment, is based on security requirements initially developed by Visa with expert support, and modified with field experience. Its purpose is to promote understanding of data security fundamentals and to recommend enhancements for existing security practices.

Entities that implement the controls outlined in this document can benefit in many ways. When applied properly and consistently, these controls can help:

- **Gain a competitive edge** – Consumer studies show that trust is a key factor in the card-not-present environment. Customers seek out merchants that they feel are “safe.” Confident consumers are loyal customers. They come back again and again, as well as share their experience with others. The result is more customers and a stronger presence in the marketplace.
- **Increase revenue and improve the bottom line** – Appropriate data security protects your customers, limits risk exposure, and minimizes the losses and operational expense that stem from compromised cardholder information. The bottom line depends on better data security.

- **Maintain a positive image** – With the incredible growth of the Internet information security is on everyone’s mind...including the media’s. Data loss or compromise not only hurts customers, it can seriously damage a business’s reputation. Protecting sensitive information builds both a solid business and a good reputation.

Data security applies to everyone in the payment system, as outlined in the *Visa U.S.A. Operating Regulations*. However, it is not reasonable to apply the same requirements across the board, nor would it be possible for Visa U.S.A. to manage such a broad compliance effort. Therefore, Visa U.S.A plans a phased program to address the various acceptance channels (including card-present), as well as various kinds of payment system participants.

The requirements and best practices in this first document pertain specifically to any and all “card-not-present” entities that process cardholder data via the Internet or mail/telephone. Thus, they apply to merchants and associated agents or servicer providers, such as processors, gateways, Internet service providers (ISPs), “master merchants,” e-malls, independent sales organizations (ISOs), credit card protection providers, rebillers, hosts, merchant “enablers,” and so on.

► **Who Should Read This Document?**

This document contains three general parts. Each part will be of primary interest to a specific audience, as follows.

<i>Executives</i>	(Part 1) An executive summary of data security requirements and an overview of the Visa U.S.A. Cardholder Information Security Program. Intended for senior management and those who need quick, high-level information about the program.
<i>Managers</i>	(Part 2) A more detailed explanation of program best practices along with operational suggestions. Intended for managers responsible for meeting program requirements at a service provider or merchant, or for anyone needing more detailed information.
<i>Technical Staff</i>	(Part 3) Appendices that provide additional detail about firewalls and cryptography. You will also find a glossary and references for further reading. Intended for security specialists and anyone wanting additional technical information.



Cardholder Information Security Program Overview

The electronic storage and transmission of account information opens new doors for compromise. The primary purpose of the Cardholder Information Security Program is to help entities prevent the abuse of cardholder information.

This booklet covers principles that Visa will require service providers and merchants to follow to protect the cardholder data entrusted to them. Each of these principles is supported by methods that field experience suggests may satisfy the requirement. Visa may accept alternate practices that can be demonstrated to provide cardholder information the same or higher level of protection.

In addition, as technology, market, and regulatory conditions evolve, new measures may become necessary to meet the challenge of providing acceptable levels of protection for cardholder information.

▶ What Needs to be Protected

“Account and Transaction Information” refers to data required to process Visa transactions. Specifically, this information includes:

- Any information used to authenticate a Visa payment transaction, such as payment card number, payment card expiration date, Personal Identification Number (PIN), Card Verification Value (CVV), Card Verification Value 2 (CVV2), passwords, pass phrases, digital certificates, and biometric authentication mechanisms.

Note: *Visa U.S.A. Operating Regulations* specifically state that CVV2 and magnetic stripe data may not be stored subsequent to authorization of a transaction.

- Any information obtained during the processing of a Visa payment transaction that identifies individual consumers and their purchases. This information includes consumer name, purchase description, purchase amount, and other details of the Visa transaction.

▶ Key Roles and Responsibilities

Within the program, the following players have major roles and responsibilities:

Visa

Role

- Establish requirements and guidelines based upon industry best practices.
- Establish and administer a reasonable and effective monitoring program.
- Conduct training to help acquirers, merchants, and service providers understand and apply these requirements and guidelines.

Responsibility

- Establish reasonable requirements and guidelines that enhance the protection of cardholder information.
- Respond to feedback from the marketplace in developing future enhancements and directions for the program.

Acquirers

Role

- Provide the primary link between Visa and the merchant and service provider community.
- Hold financial responsibility in the Visa system for the activities of associated service providers and merchants.

Responsibility

- Protect cardholder data from misuse/abuse.
- Retain legal control of proprietary information when outsourcing administration of information assets, networks, or data.
- Use limited, “need-to-know” access where a service provider administers information assets, networks, or data.
- Provide this document to their Internet and MO/TO service providers and merchants.
- Direct merchants to provide this publication to their service providers.
- Help service providers and merchants understand and apply these requirements and best practices.
- Reference the protection of cardholder information and compliance with the Cardholder Information Security Program in contracts with service providers and merchants.
- Work with service providers and merchants to correct any identified security deficiencies.

Service Providers and Merchants

Role

- Guardian of cardholder information

Responsibility

- Comply, at minimum, with the high-level requirements of this program.
- Provide a copy of this publication or its information to any service provider contracted to handle Visa cardholder information.
- Retain legal control of proprietary information when outsourcing administration of information assets, networks, or data.
- Use limited, “need-to-know” access in cases where a business agreement allows system administration of information assets, networks, or data.
- Reference the protection of cardholder information and compliance with the Cardholder Information Security Program in contracts with other service providers and merchants.
- Promptly correct any identified security deficiencies.

▶ Program Timeline

The program emphasis through April 2001 will be on awareness and education. Visa plans to offer workshops and training seminars throughout the United States, as well as online. These sessions will allow Visa to clarify the program and you to provide feedback. Once this introductory phase is complete, Visa will begin verifying compliance in May 2001.

▶ Compliance and Monitoring

Visa’s data security requirements apply to all service providers and merchants, regardless of size, working with card-not-present transactions. However, the vigilance and detail with which Visa verifies compliance will be scaled based on several risk factors, such as the number of accounts stored or processed. The measurement and monitoring process for the proverbial “mom & pop” merchant, for example, might be as simple as completing an on-line self-assessment checklist. For those handling the largest volumes of cardholder information, such as gateways or processors, Visa may require more formal assurance of compliance and additional monitoring through on-site reviews, intrusion-detection testing, and ongoing firewall adequacy monitoring.

On-site reviews are worth special mention, as they are already an important part of the compliance effort. The review process provides the higher-risk entity with an independent review of its ability to protect cardholder information. Where appropriate, the review will document changes required to protect cardholder data.

In September 2000, the on-line self-assessment questionnaire will be available on the www.visabrc.com website. Service providers and merchants can use the questionnaire to test themselves and to make any needed process changes before formal monitoring begins in May 2001.

September 2000 through April 2001	May 2001 forward
Self-Assessment	Formal Compliance

Why comply?

Some readers might wonder why they should adhere to Visa's requirements and best practices. Beyond statements of implicit liability in the *Visa U.S.A. Operating Regulations*, avoiding the unwanted media attention that results from a hacking incident may be the greatest incentive. Improving profitability depends on better data security. Proper safeguards limit exposure and minimize expense from compromised cardholder information. (Note that information theft may also result in regulatory violations and cause you legal problems.)

And while financial damages are bad enough, perhaps the more serious result of a data compromise is the negative impact on your greatest asset: your reputation.

Realistically, savvy entities in the "e-space" and card-not-present environments already adhere to Visa's requirements and, more than likely, exceed them. But, for organizations growing into these areas, it's important to recognize that the marketplace demands immediate assurance of your ability to protect confidential information.



Executive Summary

Program Requirements

At the highest level, the Cardholder Information Security Program consists of the “Top 10” logical requirements for protecting Visa cardholder information:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
2. Keep security patches up-to-date.
3. Encrypt stored data.
4. Encrypt data sent across open networks.
5. Use and regularly update anti-virus software.
6. Restrict access to data by business “need-to-know.”
7. Assign a unique ID to each person with computer access to data.
8. Don’t use vendor-supplied defaults for system passwords and other security parameters.
9. Track access to data by unique ID.
10. Regularly test security systems and processes.

Two additional requirements pertain to administrative and physical security issues:

11. Maintain a policy that addresses information security for employees and contractors.
12. Restrict physical access to cardholder information.

Note that some of these requirements may have underlying details, or sub-requirements, that apply only in certain circumstances or to higher-risk entities. Higher-risk entities could include Internet gateways, Internet

Service Providers, or merchants handling significant numbers of accounts. (“Significant” will be defined with the help of the Acquirer and merchant communities.)

“**Part 2: Requirements**” addresses these 12 requirements in more detail. Each requirement is supported by a list of best practices. Best practices are some of the ways others in the field have addressed the requirement.

As stated earlier in this booklet, acceptable practice for safeguarding cardholder information is not limited to these lists. Alternatives that achieve the same or greater level of protection may also be appropriate.



Requirements

Introduction

For each of the requirements listed in Part 1, this section contains specific measures or conditions that must be met. In addition, we've included best practices used by your peers to achieve the same or greater protection for cardholder information.

Remember, Visa may also be satisfied with alternate practices that are appropriate to your environment.

Logical Data Security

Logical, or systems-related, controls are a vital part of a strong cardholder information protection program.

Such controls include safeguards against unauthorized network access, use of encryption, identifying and authenticating users, and regular verification of security capabilities.

This chapter describes the ten logical security requirements central to the Cardholder Information Security Program.

Requirement 1:

Install and maintain a working firewall to protect data accessible via the Internet.

A firewall is a set of rules set up by a business to control the information that can go into and out of its network. All databases containing cardholder data must be protected by a firewall that restricts outside connections. Such connections include the Internet and direct, dial-up access to your private network.

The firewall must have the following characteristics:

- The firewall must prevent packets from external networks from entering the internal network.
- The router containing the firewall must not broadcast internal network addresses to the outside network.
- All DMZ and e-commerce standards must conform to the merchant's system configuration standard type and must additionally have specific enhancements, as noted below:
 - There can be one application only per system. In the event of system failure or security failure, this reduces the impact on other business.
 - The host system should contain the minimum hardware and software required to perform its function.
 - All administrative access must be encrypted.
 - No implied system trust will be permitted between the DMZ and e-commerce systems.

For more information related to firewall security, see Appendix A.

Requirement 2:

Keep security patches up-to-date.

All systems must have the latest vendor-supplied security patches installed in a timely manner.

Best Practice:



Follow change-control procedures for all software modifications processing and storing cardholder information.

Requirement 3:

Encrypt stored data.

Scrambling, or encrypting, data is an excellent way to ensure privacy. Encryption requirements include:

- Cryptographic systems must not rely upon any one particular approach. Diversification makes your system that much more flexible and harder to break.
- Cryptographic processing isolation must ensure that no secret data can be disclosed.

- Use Triple-DES encryption or other strong cryptography. This means symmetric key lengths greater than 100 bits or asymmetric key lengths of 768 bits or greater.
- Use only approved devices to process cryptographic material, such as keys. This ensures that no secret data is divulged or corrupted.
- Don't store keys in a public place. Use hardware systems with anti-tamper enclosures to store keys; software products may be used depending on circumstances.
- Ensure all cryptographic systems conform to applicable international and national standards and all legal and regulatory controls.

Best Practice:

Use "split knowledge" or "dual control" to preserve system security.

For more information related to encryption security, see Appendix B.

Requirement 4:

Encrypt the transmission of cardholder information across open networks.

When transmitting data across networks, always use an encryption technique, such as Secure Sockets Layer (SSL), to make cardholder information impossible to read. Specifically, do not allow unencrypted e-mail to be used to send cardholder information.

Best Practice:

Require secure remote access to cardholder data using the following procedures:

- Authenticate access to cardholder data requested from outside of the merchant's processing environment. In other words, make sure you really know who's asking.
- Do not allow external requests for information to directly access internal systems or data. For example, when your site receives an external request, the security system should first authenticate the requestor, pass the request itself to the internal system, receive the answer, then return the data to the requestor.
- Prevent external users from accessing any application or system within your processing environment.
- Use dial-in modems for maintenance; power-off or disconnect them except for coordinated maintenance events.
- Define strong authentication, such as dial-back controls, dynamic passwords, or token-based authentication, for remote access devices.

Requirement 5:**Use and regularly update anti-virus software or programs.**

Anti-virus mechanisms must be kept current, run on a regular basis, and capable of generating audit logs.

Best Practices:

- Have management review anti-virus audit logs at least weekly.
- Follow change-control procedures for all hardware and software modifications processing and storing cardholder information.

Requirement 6:**Restrict access to data by business need-to-know.**

The principle of “least privilege” restricts data access based on a user’s need-to-know. The more access there is to cardholder information, the less control you have.

To promote need-to-know access:

- Institute a formal process for approving all external network connections.
- Limit firewall administration to authorized staff.
- Properly dispose of cardholder data once it is no longer needed.

Requirement 7:**Assign a unique ID to each person with computer access to data.**

Uniquely identify all users prior to allowing access to cardholder information and system resources.

Authenticate users through at least one of the following methods:

- User name and password
- Certificates
- External token devices
- Biometrics

Best Practices:

Authenticate and control passwords through the following processes:

- Control the addition, deletion, and modification of user IDs, credentials, or other identifier objects.
- Distribute password procedures and policies to all users who have access to cardholder information.
- Transmit passwords in a one-way encryption format so as to protect the authentication of the user.
- Do not permit group passwords.
- Require a unique identification and password for each user accessing the system.
- Change user passwords at least bi-monthly.
- Use at least six-character passwords containing both numeric and alphabetic characters.
- Do not allow new passwords to be the same as any of the previous four passwords used.
- Require the user to re-enter the password to re-activate the terminal if the session has been idle for more than 15 minutes.
- Do not allow a specific user ID to log on more than once at the same time; in other words, do not allow simultaneous sessions.
- Have the authentication mechanism prevent “play-back” and masquerade attacks when external requests for customer data are made.
- Limit repeated attempts to establish a false identity (or to use a valid identity in an unauthorized manner) by locking out the user ID (disabling it for a preset time without disabling the terminal).

There is a special requirement of passwords worth individual mention:

Requirement 8:

Don't use vendor-supplied defaults for system passwords and other security parameters.

Vendor defaults are known to a wide range of people. Change them immediately.

Requirement 9:

Track all user access to data by unique ID.

Audit trails are records of activity used to reconstruct events and establish accountability. Audit trail information is critical to any data-related investigation.

- You must be able to link all actions and processes to an active user or system.

- You must implement automated audit trails to reconstruct system events and user actions. Audit trail entries for each recorded event must include the following information:
 - User identification
 - Type of event
 - Date and time stamp
 - Success or failure indication
 - Origination of event
 - Identity or name of affected data, system component, or resource
- The audit trail should be able to reconstruct the following system events:
 - Access to all audit journals
 - Invalid physical and logical access attempts
 - Use of identification and authentication mechanisms
 - Initialization of the audit logs
 - Deletion of objects
 - Actions taken in response to the compromise of cryptographic keys
 - Changes in the custody of keys and custody of devices or media holding keys
 - All encryption key management operations:
 - system initialization
 - key generation
 - key use
 - key storage (back-up and archiving)
 - key destruction
 - key custodian actions
 - certificate generation
 - certificate validation
 - key exchange (import and export)
- The audit trail should be able to reconstruct the following user actions:
 - All actions taken by any individual with access to the system
 - Introduction of objects into a user's address space

Best Practices:

- Supplement automated audit trails with manual back-ups.
- Retain audit trail history files for a period consistent with effective use and legal regulations (usually not less than six months).

Requirement 10:**Regularly test security systems and processes.**

Test regularly to ensure that security controls, limitations, network connections, and restrictions are working to stop or identify unauthorized access attempts.

Best Practices:

- Test your systems at least daily.
- Specifically test your security patches to ensure they provide the expected level of protection.
- Have your systems tested by an independent entity each month.
- Have systems capable of alerting personnel if compromise is suspected.

Administrative Data Security

All too often, Visa has found that fraud or compromise can be traced to either a current or former employee. Industry experts routinely note that some 70 percent of fraud can be attributed to internal compromise. This issue is one of the most difficult against which service providers and merchants must protect themselves.

Hiring the right employees, educating them about the importance of safeguarding data, and monitoring access to sensitive information are key principles in protecting cardholder data.

This section notes the requirement and several best practices that address these principles.

Requirement 11:**Maintain a policy that addresses information security for employees and contractors.**

A good information security policy encompasses the following actions:

- Include an information security policy as part of their overall business objectives.
- Publish the company's security policies, risk control objectives, standards, and requirement details.
- Publish procedures and controls that ensure daily operations consistent with industry "best practices" and Visa requirements.
- Clearly define information security responsibilities for employees.

Best Practice:

Give an individual or team specific responsibility for managing information security.

Many of your peers have individuals or teams responsible for:

- Establishing, documenting, and disseminating security policies and procedures.
- Administering user log-on IDs and passwords/authorizations, including user changes and terminations.
- Monitoring and controlling all access to data.
- Addressing all information security incidents.

Best Practice:

Make employees aware of the importance of protecting cardholder data.

Many of your peers:

- Educate employees about their cardholder information security responsibilities through posters, letters, memos, meetings, promotions, and so on.
- Have employees sign a document indicating that they have read and understood the contents of the security policy manual.

Best Practice:

Screen employees with access to data to limit the possibility of an "inside job."

Ensure that applicants for positions with access to cardholder information are not undesirables or in financial difficulty.

Many of your peers:

- Conduct criminal background checks.
- Don't hire individuals convicted of a felony, where permitted by applicable law.
- Perform credit checks.
- Verify applicant information through a social security number or other national registration number.
- Verify previous employment.
- Periodically re-review current employees with access to cardholder information.

Best Practice:

Immediately discontinue terminated employees' access to sensitive information.

These individuals have no further need to access cardholder information.

Many of your peers review a checklist that includes:

- Notification of termination to all concerned
- Recovery of proprietary property, documentation, and/or information
- Recovery of identification badges
- Retrieval of computer and communications equipment
- Retrieval of keys to restricted areas
- Retrieval or blocking of corporate payment cards
- Retrieval or blocking of corporate phone cards
- Retrieval or blocking of internal/external agent/affiliate access cards
- Timely deletion of employee computer log-on IDs
- Termination of remote data access
- Changes to lock combinations for vaults or data safes containing cardholder information (if terminated employee was previously granted access)

This same checklist can also help reconcile data accesses and account for property when an employee transfers between jobs.

► Physical Data Security

Protecting data from unauthorized physical access is a vital part of a strong cardholder information protection program. Although Internet-related security is of tremendous importance, you still need to keep unauthorized individuals from snooping around your filing cabinets. Strong physical controls can help you protect papers, diskettes, or even computer equipment.

This section notes the requirement and includes several best practices that address this principle.

Requirement 12:

Restrict physical access to cardholder data.

Best Practice:

Distinguish between employees and visitors or outsiders, especially in areas where cardholder information is accessible.

You should be able to easily determine those with permission to be in physical proximity to sensitive information. The larger the service provider or merchant, the more critical this distinction will be.

Many of your peers:

- Identify and authorize visitors before they enter an area where cardholder data is accessible.
- Give visitors badges that identify them as non-employees (when there are more than 25 employees).
- Require visitors to wear badges at all times and return them when leaving.
- Verify that vendor personnel are employed by a vendor with whom you have a current contract.

Best Practice:



Restrict or closely monitor outsiders' presence in areas where cardholder information is accessible.

Many of your peers:

- Restrict vendors or visitors from areas where cardholder information is processed/maintained.
- Accompany visitors or vendors if they must enter restricted areas.

Best Practice:



Physically secure all paper and electronic media (such as computer, networking, and communications hardware) containing cardholder information.

Many of your peers:

- Keep computer equipment in a secure location.
- Allow access only to those employees whose jobs require access.
- Keep telecommunications equipment and lines in a secure location.
- Restrict access to data security software to personnel approved by management.
- Limit employee access to documents/files that contain cardholder information.
- Develop and maintain policies and procedures that control the copying of cardholder information.
- Follow special procedures to protect documents and media containing cardholder information, such as:

For Hardcopy Documents:

- Place cardholder information not being worked on in locked cabinets in a secure location.

- When document processing is complete, log hardcopies and record the retention dates.
- Establish document storage policies for processed orders, such as storing retained records in a secure area and destroying them at the end of the retention period.

For Magnetic/Optical Media (diskettes, hard drives, tapes, CDs):

- Store all electronic cardholder information maintained on transportable media in a secure location approved by management.
- Encrypt cardholder data on any portable media, such as CDs or diskettes, **not** stored in a secure location.
- Restrict access to electronic cardholder information maintained in computer files/databases.
- Encrypt cardholder data stored on any handheld portable devices, such as PDAs, palmtops, smart phones, or laptop PCs.
- Back up magnetic and optical media, as it is easily duplicated and equally easy to “misplace.” These risks may be addressed as follows:
 - Create and document off-site data storage procedures for all cardholder information files.
 - Establish retention dates for each type of file.
 - Account for all data files by serial number, file name, date and time, and retention date before removing for back-up.
 - Count and check files returned from off-site to ensure that all are present.
 - Purge and degauss cardholder information from returned media before any reuse.

Best Practice:



Take precautions to guard against data compromise when taking orders over the Internet, or by telephone, mail, or fax.

Many of your peers follow special procedures to secure data when taking orders over these acceptance channels:

For Internet Orders:

- Remove the cardholder information and store it in a limited-access electronic file/database once an order has been processed.
- Secure the extracted data on a computer separate from the device used for the Internet web site.
- Do not solicit or send cardholder orders/information using unencrypted e-mail.

- Allow unencrypted e-mail for acknowledging the receipt of an order only as long as no cardholder information is included other than the e-mail address and name.

For Telephone Orders:

- Ensure that telephone representatives ask callers for appropriate cardholder information only.
- Have representatives work from a script that has been approved by management.
- Periodically monitor telephone calls to ensure that representatives are not obtaining more cardholder information than necessary.
- Ensure that there is accountability for all cardholder information transcribed to hardcopy forms.
- Store all documents in a restricted area.

For Mail and Fax Orders:

- Collect and account for all documents containing cardholder information, such as order forms and carbons.
- Process documents containing cardholder data in a restricted area.
- Place any fax machines used to take orders or to share cardholder information in a restricted area.

Best Practice:



Maintain strict control over how data is distributed.

Many of your peers:

- Limit distribution of cardholder information and validate its receipt.
- Review the need for such distributions quarterly.
- Label as “confidential” any kind of media containing cardholder information prepared for internal or external distribution.
- Encrypt any magnetic media prior to distribution.
- Send any media by overnight courier.
- Have management approve all media movement from a secured area, especially media distribution to individuals.

Best Practice:



Maintain strict control over stored data and access to it.

Many of your peers:

- Properly inventory and securely store media.

- Establish and monitor data-retention limits to ensure that the only cardholder information maintained is that required by law or a governing organization.
- Maintain recurring payment data in a secure environment for only as long as required; then promptly destroy it.
- Perform a quarterly inventory audit to verify that no unneeded cardholder information is maintained.
- Create a schedule for all retained electronic cardholder information that identifies when data should be:
 - Removed from production environment
 - Archived to on-site storage
 - Archived to off-site storage in a certified facility
 - Destroyed/purged

Best Practice:

Destroy data when it's no longer needed for business or legal reasons.

A strong cardholder data security program includes the destruction of information for which there is no longer a business need. Such information should be destroyed completely.

Many of your peers:

- Shred or incinerate hardcopy materials.
- Purge, degauss, shred, or otherwise destroy electronic media so the cardholder data cannot be reconstructed.
- Establish a procedure to verify that destruction has taken place and no residual data remains.
- Accompany the material and witness its complete destruction if destroyed at an off-site location.



Firewall Complexes

This appendix defines the characteristics of required firewall security mechanisms.

► Firewall Definition

Essentially, a firewall is a set of rules a business uses to control the data that goes in and out of their systems. For the most part, you can think of a firewall rather like a security guard at a front desk that checks visitor IDs, thereby controlling and logging access to a building.

A properly designed firewall restricts all data and services to the bare minimum required to perform a specific function. The firewall blocks all traffic that is not implicitly required to complete a specific transaction. Further, the firewall may be used to encrypt traffic to and from the endpoints of a networked connection.

The firewall mechanism enforces the security stance noted above. The firewall specification stance can be stated as follows.

A firewall mechanism is to be put into place such that all electronic cardholder data is protected from unauthorized access during all phases of its life, from generation to destruction, such that it cannot be compromised, released to any unauthorized entity or otherwise have its confidentiality or integrity placed at risk. The firewall mechanism must be built and maintained using the model of least privilege. All access are to be on a need-to-know basis, and more importantly, all access to cardholder data will be restricted to personnel who need to access said data to perform their stated job function only. Any service or access not specifically required and documented will be denied.

The areas of main emphasis for firewall protection are:

- Firewall Attributes
- Firewall Security Standards
- E-commerce DMZ Security

► Firewall Types

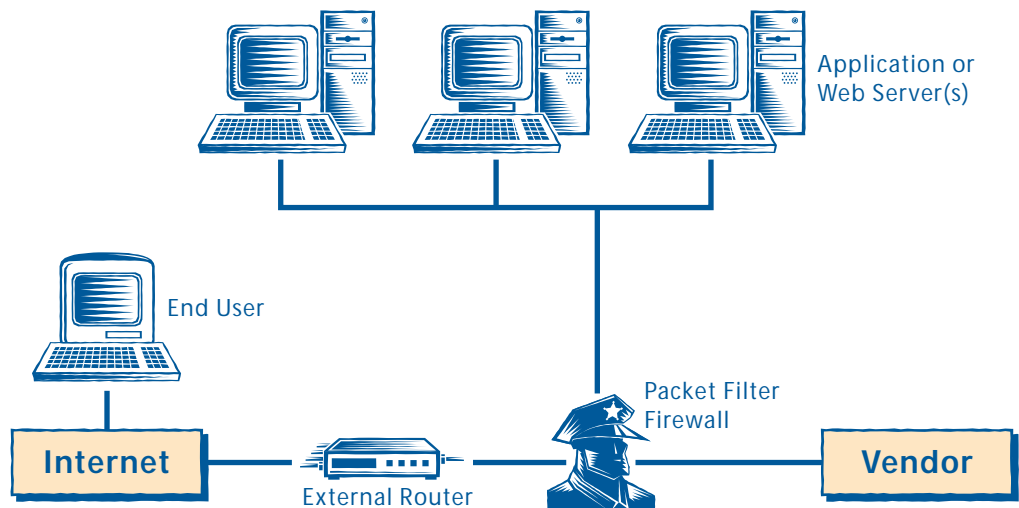
An Internet firewall is designed to restrict data and data types to the minimum set required to perform a function. There are three basic types of firewalls in use on the Internet today.

Packet Filter

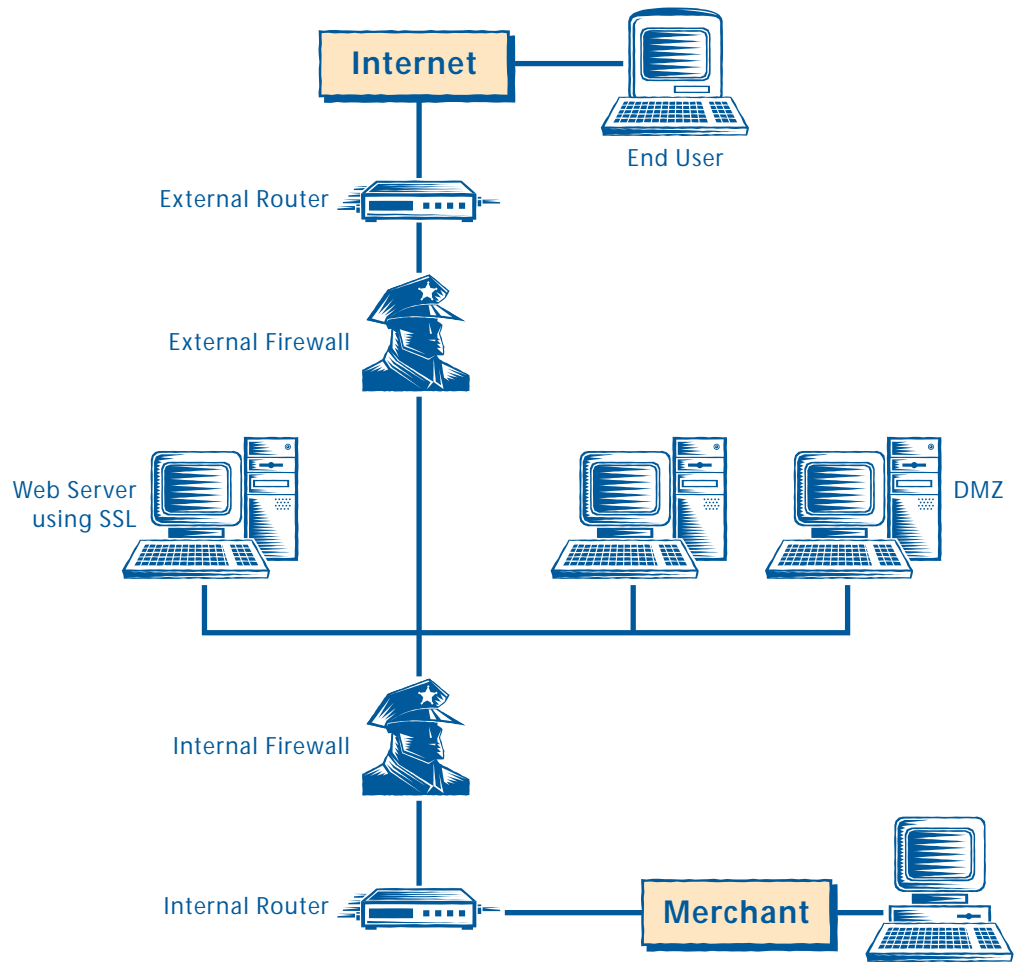
A packet filter firewall examines each individual message (IP packet) and, based on the packet filtering rule set, decides to pass or drop the packet (additional functionality may include encryption). Packet filter firewalls are commonly the easiest to configure for new services, and allow the fastest communications. Packet filter firewalls commonly filter on source and destination IP address, and do not authenticate down to the user level.

The rules that make up a packet filter reside as software code on pieces of hardware called routers. Routers are analogous to your local post office. They are placed at network endpoints and throughout the Internet to relay packets to the appropriate destinations. They also, of course, control which packets can be sent to which destinations.

Example A. Typical Packet Filter Firewall and DMZ system hosting applications



Example B. Typical Packet Filter Firewall using external as well as internal Firewall on separate hardware



Proxy

A Proxy firewall acts as a secure gateway that breaks the communication path between networks. The proxy authenticates the information and passes only specific types of information to/from the secure side of the proxy. On the plus side, proxy firewalls are inherently secure because they pass only known service types and are able to authenticate the user to a fine granularity. On the down side, adding new services can be cumbersome.

Hybrid

A Hybrid (or “complex”) firewall uses both packet filtering and proxy firewalls to give the best of both worlds.

In all three types of firewall, it is important to understand that the firewall is simply a security mechanism, and does not house any other application or cardholder data. All applications (web server or transaction application) are housed on separate hardware which is commonly on an isolated network segment (DMZ) that is protected by the firewall system.

Firewall Security Standards

The characteristics of a recommended firewall configuration are:

- The only service type that should be passed through the firewall to the Visa merchant system should be HTTP (port 80) and any encrypted session for the transaction (commonly SSL port 443).
- Further HTTP (port 80) should be re-directed to an encrypted session (commonly SSL port 443) such that all cardholder transactions are done through the encrypted connection. This ensures confidentiality of the entire transaction.
- To enforce logical system security, the firewall system should be configured as follows:
 - A separate DMZ may be used to house the Visa merchant system.
 - No other services or other business ventures should reside on the same DMZ network segment as the Visa merchant system.
 - Encryption (such as SSL) should be used for all communications between the end user and the merchant system (see encryption standard).
 - Network encryption (VPN) may be used between any merchant system and any back-end database.
 - No back-end database should store cardholder information longer than is necessary to complete the purchase transaction.
 - Access to any database holding cardholder information should be restricted to the merchant and any administrative support staff or other entities as determined by the Acquirer or merchant.

Cryptographic and Key Management Mechanisms

Cryptographic controls assure entities that processed or stored data will be protected from unauthorized access. Properly implemented, Key Management procedures protect encryption access keys from being improperly displayed or disseminated.

This appendix provides the guidelines and standards to which entities using any cryptographic system should adhere.

Good industry practices strongly recommend that cardholder data be encrypted when resident in the merchant's/agent's database.

The areas of main emphasis for cryptographic management include:

- Cryptographic System Criteria
- Key Management Controls

▶ Cryptographic System Criteria

The implementation and use of a cryptographic system must be based upon the characteristics noted here.

- Merchant systems using cryptography should be designed so they are not reliant upon any one particular implementation approach for the cryptographic systems utilized.
- Cryptographic processing isolation should be enforced such that no keys or intermediate cryptographic results can be disclosed beyond the defined cryptographic boundary.
- The use of approved devices for the processing of cryptographic material, such as keys, must be enforced to ensure that no secret data, key, or intermediate cryptographic results are divulged or corrupted.

- Symmetric or secret-key cryptographic systems which use a specific key for both encryption and decryption operations should be used when a one-to-one relationship exists between two parties, and when a high level of security is required for relatively large amounts of data.
- Asymmetric or public-key cryptographic systems which use a public/private pair (one for encryption and another for decryption) should be used where a one-to-many relationship exists between multiple entities.

The characteristics to be considered when evaluating and selecting a cryptographic system include:

- What specific security features are required? Are confidentiality and/or integrity required?
- What are the primary operations requirements? Will cryptography be used for entity authentication, transmission, or storage security?
- What is the format and amount of data that is controlled and encrypted? Is the data static in nature or does it change constantly?
- How many users require authentication? Is there a limited population of users or will it grow constantly?
- What are the speed and performance requirements for the operations? Is the system dependent on high-performance needs or not?
- What level of security is needed? Must data be protected for the short term or long term? This may dictate the key length (strength). A strong cryptographic system should offer a large key space (in other words, be able to support sufficiently long keys relative to the needs of a merchant).
- Are solutions commercially available and does the vendor provide support? Can the merchant support their systems internally or is support contracted out?
- Other technical considerations are:
 - Does the cryptographic system produce apparently random results?
 - Does the cryptographic system resist known attacks?
 - Has the cryptographic system been publicly scrutinized for a long period of time?
 - Does the cryptographic system use publicly available or proprietary algorithms or features?
 - If the cryptographic system supports key back-up or key escrow, who controls the keys?

▶ Key Management Controls

The security and integrity of a cryptographic system relies upon the security and integrity of the keys used with it. For this reason, key management plays a significant role in the overall implementation and use of those systems.

Beyond the selection of a cryptographic system a merchant should be concerned with the initial implementation and ongoing maintenance of the system. The objective of key management is to ensure that the cryptographic system is implemented and used with an appropriate level of security and integrity.

Key management standards direct the implementation, use, and administration of cryptographic keys throughout their life cycle. These key management controls ensure the security and integrity of cryptographic systems.

Entities must ensure that any cryptographic application, system or other solution they implement complies with these principles.

The key management standards are:

- Access to keys
- Random key generation
- Allowable key forms
- Dual control
- Split knowledge
- Audit trails
- Intended key usage
- Key compromise
- Compartmentalization of risk
- Cryptographic strength
- Key management documentation

Access to Keys

Controls limiting access to keys include:

- Access to keys or components must be on a need-to-know basis.
- Keys must be protected against both disclosure and misuse.
- Keys must be accessible only to the fewest number of key custodians necessary to enable their effective use.
- Unauthorized modification, substitution, or replay of keys must be prevented.
- Keys must be used only when there is a reasonable assurance that their integrity is assured.

- Keys must exist in the fewest possible locations or forms necessary to enable their effective use.
- Systems utilizing keys must prevent the disclosure of any key that has been used to encipher any still-secret or confidential data or used to provide an authentication value (such as a MAC) for data.
- The factors of the public modulus and the private exponent in a public key cryptosystem must always be kept secret and protected from disclosure.

Random Key Generation

The characteristics of random key generation are:

- Symmetric keys must be generated such that they are unique between entities.
- Keys must be generated using an appropriate random or pseudo-random process.
- The key-generation process must ensure that it is not possible to predict any key or determine that certain values are more probable than others.

Allowable Key Forms

Encryption keys must exist in a limited number of states to reduce the opportunity to compromise them.

- Cleartext keys must exist within a qualified cryptographic device or where their compromise will only affect a single user.
or
- Cleartext keys must exist as at least two separate components with each controlled by a separate key custodian and using dual control and split knowledge. Key components must never be combined via concatenation. Every active bit of a resultant key must be a function of every active bit of each key component. Note that these requirements do not mandate the specific media for components.
- Keys may exist as threshold scheme shares or components, but each component must be controlled by a separate key custodian using dual control and split knowledge. The minimum number of total shares must be three (3) or greater and the minimum threshold must be two (2) or greater.
or
- When not in protected memory or as components, keys must be enciphered by another key of equal or greater cryptographic strength.
- Cleartext asymmetric public keys must exist, until validated by the recipient, as either signed certificates or MAC'ed with a key of strength equal to a 128-bit DES key, such that their integrity and validity can be tested externally.

Dual Control

Secret symmetric or private asymmetric keys, or their key components, must always be managed and under the control of at least two key custodians.

The characteristics of dual control are:

- No one person shall have the ability to obtain, determine use, or alter a cleartext key or more than one cleartext key component.
- Dual control must be used for all keys and components regardless of their state or form.
- Dual control must utilize two or more separate entities (usually persons), operating together, to protect sensitive functions or information.

Split Knowledge

Secret symmetric or private asymmetric keys must always be managed by at least two key custodians who do not have knowledge of the each other's keys or key components.

The characteristics of split knowledge are:

- Cryptographic keys, when in multiple component form, must be entrusted to and controlled by more than one key custodian, where one custodian can never learn or know any other key component but their own.
- Split knowledge is a condition under which two or more parties must separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key.
- Different individuals must be responsible for different functions, so that there is a clear separation of duties.
- Key custodians must not be responsible for the design, development, or implementation of facilities upon which they rely for performing the key custodial functions.

Audit Trails

All key management activities should be logged and adequate information maintained such that all key management processing can be reviewed.

The characteristics of audit trails are:

- Audit trails must be generated and maintained for all actions that occur within the life cycle of a cryptographic key or key components.
- Audit trails must kept, at minimum, for a period of time greater than the life of the cryptographic key or key components that they cover.
- Audit trails must include enough data to enable a complete reconstruction of all key management activities, including when, where, why, by whom, and how all events took place.
- Audit trails must be secured so that they cannot be altered.
- Audit trails must be reviewed periodically to detect violations of policy.

Intended Key Usage

Keys must only be employed for specifically defined functions. This is also known as “key separation.” Separation helps isolate any corruption that may occur from the compromise of a cryptographic key.

The characteristics of intended key usage are:

- All keys must be associated with unique and identifiable functions.
- All systems that use keys must be capable of determining the specific function of a key such that they cannot be used for unauthorized or alternate processes.
- All cryptographic keys must only be used for the purpose for which they were intended.
- All cryptographic keys must be associated with a specific protocol or set of related protocols for which they are exclusively used.
- Production keys must not be present or used in test systems.

Key Compromise

Procedures and mechanisms must exist to manage the suspected or known compromise of cryptographic keys or key components.

The characteristics of key compromise prevention are:

- Unauthorized attempts to disclose, access, use, modify, substitute, or restore a key known or suspected of compromise must be precluded or detected.
- All systems and facilities that use cryptographic keys must be capable of detecting the compromise or use of a key for unauthorized purposes.
- A key suspected or determined to have been used for any other than its intended purpose must be replaced.
- Mechanisms must exist to prevent and ensure the detection of a key compromise that may occur through various attacks.
- A cryptographic key suspected of being compromised or of unknown authenticity, security, or integrity must be discarded and replaced. Any key protected by this key must also be replaced.

Compartmentalization of Risk

Mechanisms should exist to isolate the exposure from the compromise of a key.

The characteristics of compartmentalization of risk are:

- Keys must be used only where compromise adversely affects the fewest possibly entities. In particular, symmetric keys must be shared between no more than two entities and private keys of asymmetric systems shall never be shared.
- A compromised key must not provide any information used to determine its replacement.

- A compromised key shared among one set of entities must not compromise keys shared among any other set of entities.
- All keys hierarchically under a compromised key must be discarded and replaced.
- Knowledge of keys generated at one time must not compromise keys generated at another time.

Cryptographic Strength

Keys must never be employed past their useful life.

The characteristics of cryptographic strength are:

- To prevent their potential compromise, keys must be replaced prior to the time feasibly required to determine them through cryptanalysis.
- A key must be replaced by a new key within the time feasibly required to perform a successful dictionary attack on the old key.
- A key must not be used to ensure the security or integrity of data where it is feasible to determine that key in a period of time less than the useful life of that data.
- Keys must be equivalent to a double-length DES 112-bit key when used in an ISO- or ANSI-approved Triple DES operation.
- Keys used for one-time transactions, and where the data affected can no longer be used or compromised, may be equivalent to a DES 56-bit key.

► Key Management Documentation

All key management processes and procedures must be adequately documented.

The characteristics of adequate documentation include:

- Key management processes and procedures must be sufficiently documented to enable the reconstruction of all related events, and to ensure continued, consistent application of these procedures and processes when personnel changes.
- All compromise detection, response, and recovery procedures and mechanisms must be documented.
- The identification of all key custodians, entities, and organizations necessary to perform any key management function must be documented.
- All audit, logging, and disaster-recovery procedures applicable to key management must be documented.
- The level of detail in all key management documentation must be such that no ambiguity exists and all operations and processes can be carried out in accordance to the requirements of this manual.



Data Security Vendors

This section contains a brief list of vendors that provide firewalls products and services. This list does not constitute a recommendation by Visa U.S.A.

Company	Product Name	OS
Checkpoint	FW-1	Unix and NT
Cisco	PIX	Dedicated h/w
Raptor	Raptor FW	Unix
Sun Microsystems, Inc.	EFS 3.0	Unix (Solaris)
Trusted Information Services	Gauntlet	Unix

Glossary of Terms

Alias	Also AKA (Also Known As) is an alternate identity for any entity.
Asymmetric Cryptography	See <i>Public- Key Cryptography</i> .
Audit	The independent examination of records and activities to ensure compliance with established controls, policies, and operational procedures, and to recommend any indicated changes in controls, policy, or procedure.
Authenticate	To determine that something is genuine.
Authentication	The act of verifying the identity of one or more users.
Authorization	The process of determining whether a user may use a service or access a resource.
Cardholder Information	Refers to all of the data about the cardholder and relationships to the Member (i.e., account number, expiration date, data provided by the Member, other electronic data gathered by the merchant/ agent, and so on.) This term also accounts for other personal insights gathered about the cardholder (i.e., addresses, telephone numbers, and so on), which may have been obtained from telephone conversations (MO/TO), hardcopy documents, or other communications.
Cleartext	Data that is not encrypted.
Compromise	An intrusion into a computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.

Computer Fraud	Computer-related crime involving deliberate misrepresentation or alteration of cardholder data in order to obtain something of value.
Confidentiality	Assuring cardholder data will be kept secret, with access limited to authorized individuals/operations.
Connectivity	A program or device's ability to link with other programs and devices
Cryptography	The science concerning the principles, means, and methods for rendering plain text unintelligible and for converting encrypted messages into intelligible form.
Data Security	The result of any system of policies or procedures for identifying, controlling, and protecting cardholder data from unauthorized disclosure.
DES	(Data Encryption Standard) An unclassified cryptographic algorithm used for the protection of unclassified, but confidential data.
DMZ	A software and/or hardware barrier between devices that control external data traffic and internal production databases.
Employee	Any full- or part-time staff member, temporary personnel, or consultant/vendor who is "resident" to the merchant site.
Encrypt	To scramble information so that only someone knowing the appropriate secret information/code can obtain the original data by decrypting it.
Entity	For the purposes of this booklet, any group or individual responsible for data security. An entity could be an Acquirer, a merchant, or merchant's agent.
Firewall	A system or combination of systems that enforces a boundary between two or more networks. A network firewall is a mechanism for enforcing a trust boundary between two networks.
Host	The main hardware on which software is resident.
Hybrid Firewall	A firewall that includes both packet filtering and proxy servers. See Firewall.
ISO	(Independent Sales Organization), An organization or individual that is not a Member and whose bank card-related business relationship with a Member involves: merchant solicitation, sales, or service and/or cardholder solicitation services.

Key	A value or sequence of symbols used to encrypt or decrypt data. It controls the encryption transformation performed.
Key Escrow	The procedure of giving a portion of a key to each of a certain number of trustees such that the key can not be recovered without collaboration of all trustees.
Network	The hardware that connects various hardware/software systems, enabling them to communicate.
Packet	A block of data sent over the network containing “payload” information as well as the identities of the sending and receiving locations.
Personnel Security	Policies and procedures established to ensure that all employees with access to cardholder data have the required authorizations and clearances.
Physical Security	The measures used to provide for the physical protection of resources against deliberate or accidental threats or attacks.
Plaintext	Unencrypted cardholder data.
Privacy	Protection from unauthorized disclosure of data.
Private-Key Cryptography	Both the sender and receiver of secure data use a single secret key to encrypt and decrypt data. This key is known to each party and must be distributed/controlled securely.
Protocol	An agreed-upon method of communication used within networks. A specification which describes the rules and procedures that products should follow to perform activities on a network.
Public-Key Cryptography	The type of cryptography in which part of the encryption key is publicly available and unprotected, and part of the decryption key is protected. Only a party with knowledge of both parts of the decryption key can decrypt the cipher data.
Router	A dedicated computer that connects two or more networks. Routing software uses predefined rules to forward packets from one to the other.
Security	The establishment and maintenance of measures that ensure the protection of confidential data.
Security Administrator	An individual or team of individuals formally appointed by management or an approving authority to ensure that all cardholder data is protected from unauthorized abuse or misuse.

Server	Hardware or software which accepts, processes, and stores cardholder data. As software, a server is a program which provides some service to other programs. As hardware, a server provides some services for other computers connected to it via a network.
Session	A connection between a user terminal and a computer or server that allows communication to occur.
Strong Encryption	Symmetric key lengths greater than 100 bits or asymmetric key lengths of 768 bits or greater.
Symmetric Cryptography	See <i>Private Key Cryptography</i> .
System	A computer hardware configuration including all peripheral devices.
Triple DES	Triple Data Encryption Standard, an encryption protocol using 128-bit key and provides significantly stronger encryption than does DES.
Unencrypted Data	See <i>Plaintext</i> .
Vendor	Repair staff, suppliers, and maintenance personnel including not only business suppliers, but also such services as cleaning crews, maintenance staff, repair technicians, trash collectors, vending machine maintenance, messengers/delivery personnel, and so on.
Virus	A program or a string of code that can replicate itself and cause the modification or destruction of software or cardholder data.
Visitor	A vendor, guest of an employee, service personnel, or anyone who needs to enter a facility for a short duration, usually less than three hours.

Index

Acquirer roles and responsibilities: i, 4
Administrative Data Security: 15
Anti-virus requirement: 11
Audit trail requirement: 13
Complex firewall: 26
Compliance: 5
Contractor security policy requirement: 15
Cryptographic systems:
 Criteria: 27
 Evaluating: 28
 Selecting: 28
Data requiring protection: 3
Discs, securing: 19
Employee security policy requirement: 15
Employees: Assigning security responsibility: 15
Encryption requirement: Data transmission: 11
Entity, defined: B
Executive summary: i, 7
Firewall requirement: 9
Firewall:
 Characteristics: 26
 Defined: 23
 Types: 24
Hardcopy, securing: 18
Hybrid firewall: 26
ID requirement: 12
Key management: 29
Key management standards: 29

Keys:

- Access: 29
- Audit trails: 31
- Compromise: 32
- Documentation: 33
- Dual control: 31
- Forms: 30
- Generation: 30
- Risk control: 32
- Split knowledge: 31
- Strength: 33
- Usage: 32
- Merchant roles and responsibilities: i, 5
- Need-to-know requirement: 12
- Overview: i, 3
- Packet filtering: 24
- Program requirements, summarized: i, 7
- Proxy firewall: 26
- Roles and responsibilities: i, 4
- Self-assessment questionnaire: 6
- Service provider roles and responsibilities: i, 5
- Testing requirement: 14
- Timeline: i, 5
- Training seminars: 5
- Vendor defaults requirement: 13
- Visa roles and responsibilities: i, 4
- Visitors: 17
- Workshops: 5