



Sample Security Policy for CPA Firms

If your firm accepts credit card payments, it needs to be PCI compliant. One aspect of compliance is creating a security policy for your firm.

A security policy is simply a document outlining your firm's security procedures and requirements for handling client information. It includes best practices for using technology in your office and explains how sensitive information should be stored and disposed of. Too many CPAs neglect to document their security policy because they just don't know where to start, so we're here to help.

The following sample security policy is a great starting point for your own firm. Be sure to customize it for your unique needs, distribute it to your staff, and update it regularly to maintain its accuracy. With a straightforward security policy in place, you're one step closer to running a secure, PCI-compliant business.

***DISCLAIMER:** The following Information Security Policy is intended to serve only as an example of policies and procedures for a Level 4 merchant. These policies may or may not cover every requirement outlined by the PCI-DSS. It is the responsibility of the entity utilizing this tool to ensure full compliance with PCI-DSS regulations. CPACHarge will not accept responsibility for the incompleteness or misuse of this template.*

Table of Contents

Introduction 3

Ethics and Acceptable Use Policies 3

Usage Policy 3

Disciplinary Action..... 4

Protect Stored Data 4

Restrict Access to Data..... 4

Physical Security..... 4

Security Awareness and Procedures 5

Security Management/Incident Response Plan 5

Appendix A – List of Service Providers 7

Appendix B – Employee Agreement..... 8

Introduction

This policy covers the security of company information and must be distributed to all company employees. Management will review and update this information security policy at least once a year to incorporate relevant security needs that may develop. Each employee must read and sign a form verifying they have read and understand this policy.

Ethics and Acceptable Use Policies

[Enter company name] expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to an appropriate supervisor.

Security of company information is extremely important to our business. We are trusted by our customers to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (i.e., name, address, phone number, email, Social Security number, driver's license number, bank account, credit card numbers, etc.) or company information not publicly available (i.e., clients' financial information, employee information, schedules, technology, etc.). It is important the employees do not reveal sensitive information about our company or our customers to outside resources that do not have a need to know such information.

Usage Policy

[Enter company name] expects all employees to do their best to protect client information.

[Enter company name] prohibits employees from using the following media without prior knowledge of the management team: remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs). All software installations must go through the proper channel to ensure that the correct anti-virus and security programs are in place. **[Enter company name]** does not allow the storage of personal client information on employees' home computers such as the Social Security numbers or any bank account and financial information. The use of removable electronic media is also prohibited for storing credit card information. **[Enter company name]** does not approve of any cardholder data leaving the building and the expectation is that all payments are ran onsite unless otherwise authorized.

Employees are prohibited from receiving and storing personal client information on their home computers. Employees are expected to not store company passwords on other computers that they use to conduct company business when out of the office or working remotely. The proper use of email is also expected. Employees are prohibited from emailing or utilizing chat or messaging programs to transmit personally identifiable information to or from clients or other

employees that may lead to that information being compromised. For example, it is prohibited to email Social Security numbers or credit card numbers.

Disciplinary Action

An employee's failure to comply with the standards and policies set forth in this document may result in disciplinary action up to and including termination of employment.

Protect Stored Data

Protect sensitive information stored or handled by the company and its employees. All sensitive information must be stored securely and marked as confidential until no longer needed for business reasons. Any media (i.e., paper, floppy disk, backup tape, computer hard drive, etc.) that contains sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable (i.e., shredding, degaussing, disassembly, etc.).

Credit Card Information Handling Specifics

- Destroy cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable.
- It is prohibited to store the contents of the credit card magnetic strip (track data) on any media whatsoever.
- It is prohibited to store the card validation code (3- or 4-digit value printed on the signature panel of the card) or PIN number on any media whatsoever.
- All but the last 4 numbers of the credit card account number must be masked (i.e., x's or *'s) when the number is displayed electronically or on paper.

Restrict Access to Data

Restrict access to sensitive information (business data and personal information) to those that have a need to know. No employees should have access to credit card account numbers unless they have a specific job function that requires such access.

Physical Security

Restrict physical access to sensitive information, or systems that house that information (i.e., computers or filing cabinets storing cardholder data), to protect it from those who do not have a need to access that information. Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drives, etc. All cardholder data should be labeled as confidential and securely stored. If media needs to be shipped, it will be done by a secure courier or by using a shipping method that can be accurately tracked.

[Enter Company Name] will keep, on record, all credit card order forms in a secure file for six months to cover the chargeback window. After that, all forms containing the full credit card number will be shredded and disposed.

- Media containing sensitive information must be securely handled and distributed.
- Media containing sensitive information (especially credit card account numbers and Social Security numbers) should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, incinerating, or degaussing before disposal so that it cannot be reconstructed.
- Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information.
- Password protected screen savers should always be used on any computers that may contain sensitive information.

Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following company policies and procedures address this issue.

- Hold **[enter time interval (e.g., quarterly)]** security awareness training meetings of employees and contractors to review correct handling procedures for sensitive information.
- Employees are required to read this security policy and verify that they understand it by signing an acknowledgement form (see Appendix B).
- Background checks (such as credit and criminal record checks, within the limits of local law) will be conducted for all employees that handle sensitive information.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association PCI data security standards (PCI-DSS).
- Company security policies must be reviewed annually and updated as needed.

Security Management/Incident Response Plan

The security officer is responsible for communicating security policies to employees and tracking adherence to policies. In the event of a compromise of sensitive information, the security officer will oversee the execution of the incident response plan. In the instance of suspected fraud or a breach in the system, **[Enter Name]** should be notified immediately and she will act as the security officer for **[Enter Company Name]**.

Incident Response Plan

1. If a compromise is suspected, alert the information security officer, **[Enter Name]**.
2. Security officer will conduct an initial investigation of the suspected compromise.
3. If compromise of information is confirmed, the security officer will alert management and begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers, perform the following:
 - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
 - Alert necessary parties (merchant bank, Visa Fraud Control, law enforcement)
 - Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.
 - More information:
<https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf>

Appendix A – List of Service Providers

List of Service Providers – <https://www.visa.com/splisting/>

Provider	Type	Contact	Contact Number
<i>Example: CPACharge</i>	<i>Virtual Terminal</i>	<i>Doug Johnson</i>	<i>555-555-5555</i>

Appendix B – Employee Agreement

Agreement to Comply with Information Security Policies

Employee Name: _____

Department: _____

Date: _____

I agree to take all reasonable precautions to assure that company internal information, or information that has been entrusted to the company by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand the policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

X

Employee's Signature