



# Information Security Policy



# Table of Contents

Introduction

Ethics and Acceptable Use Policies

Usage Policy

Disciplinary Action

Protect Stored Data

Restrict Access to Data

Physical Security

Security Awareness and Procedures

Security Management /Incident Response Plan

Appendix A- List of Service Providers

Appendix B - Agreement to Comply Form



## **Introduction**

This policy covers the security of CFA Society of Houston information and must be distributed to all CFA Society of Houston (CFAH) (to be known as “company”) employees (“employees” are but not limited to CFAH members-at-large, volunteers, officers and or directors as well as contractors or vendors doing business with and or representing CFAH). Management (“management” refers to any current elected officer of CFAH) 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**

CFA Society of Houston 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 in writing to our office at P O Box 56283, Houston, Texas 77256 any dishonest activities or damaging conduct to an appropriate society officer.

Security of company information is extremely important to our business. We are trusted by our members and customers to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (i.e.- 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, members or customers to outside resources that do not have a need to know such information.

## **Usage Policy**

CFA Society of Houston expects all employees to do their best to protect client information. CFA Society of Houston 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. CFA Society of Houston does not allow the storage of personal client information on employee’s home computers such as the social security number or any bank account and financial information. The use of removable electronic media is also prohibited for storing credit card information. CFA Society of Houston 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 e-mail is also expected. Employees are prohibited from e-mailing 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 e-mail 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 membership in the CFA Society of Houston.

## **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 (ex. 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 drive, 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.

CFA Society of Houston will keep on record all credit card order forms in a secure file for 3 months to cover the charge back 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 annual security awareness training meetings of employees and contractors to review correct handling procedures for sensitive information. Security awareness training will also be done for new employees and contractors shortly after they are hired or engaged.
- Employees are required to read this security policy and verify that they understand them by signing an acknowledgement form (see Appendix A).
- 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 security standards. (PCI-DSS)
- Company security policies must be reviewed annually and updated as needed.

## Security Management/Incident Response Plan

The Treasurer is responsible for communicating security policies to employees and tracking adherence to policies thus functioning as the security officer. In the event of a compromise of sensitive information, the Treasurer will oversee the



execution of the incident response plan. In the instance of suspected fraud or a breach in the system then the President should be notified immediately and he/she will act as the security officer for CFA Society of Houston.

### ***Incident Response Plan***

1. If a compromise is suspected, alert the information security officer, 2010-2011 Treasurer, Jeff Curtiss.
2. The 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

[Http://usa.visa.com/business/accepting\\_visas\\_ops\\_risk\\_management/cisp\\_if\\_compromised.html](http://usa.visa.com/business/accepting_visas_ops_risk_management/cisp_if_compromised.html).



Appendix A – List of Service Providers

List of Service Providers – review the following:

<http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf>

<b>CFAH Provider</b>	<b>Contact Number</b>
Plug & Pay Technologies, Inc.	1.800.945.2538
Affiniscap Merchant Solutions	1.866.376.0950
National Processing Company – NPC	1.800.683.2289
Retriever Merchant Solutions	1.877.479.6649
Authorize.net	1.800.455.4577



Appendix B- Employee Agreement

Agreement to Comply with Information Security Policies

Name: \_\_\_\_\_

Date: \_\_\_\_\_

I agree to take all reasonable precautions to assure that CFA Society of Houston 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 violation or suspected violations of information security policies to the designated security officer.

X

\_\_\_\_\_  
Employee's Signature