

Information Security Policy

For Offline Merchants

(Company Name)

(Date)

Table of Contents

Table of Contents	ii
Introduction.....	1
Ethics and Acceptable Use Policies	1
Disciplinary Action.....	1
Protect Stored Data.....	1
Protect Data in Transit.....	2
Restrict Access to Data.....	2
Physical Security.....	2
Security Awareness and Procedures	2
Security Management / Incident Response Plan	3
Appendix A – Agreement To Comply Form	4

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

The company 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, e-mail, 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.

Disciplinary Action

An employees failure to comply to 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 disposed of in a secure manner when 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 (shred, degauss, etc.).
- It is prohibited to store the contents of the credit card magnetic stripe (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) 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.

Protect Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e. – to a secure storage facility or across the Internet).

Credit Card Information Handling Specifics

- Credit card account numbers must never be e-mailed without using proper encryption technologies (i.e. – PGP encryption).
- Media containing credit card account numbers must only be given to trusted persons for transport to off-site locations.

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.

- Media containing sensitive information must be securely handled and distributed.
- Media containing stored 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, or degaussing before disposal.
- 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 periodic 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 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

There will be an employee of the company designated as the security officer. The security officer is responsible for communicating security policies to employees and contractors and tracking the adherence to policies. In the event of a compromise of sensitive information, the security officer will oversee the execution of the incident response plan.

Incident Response Plan

1. If a compromise is suspected, alert the information security officer.
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 hrs.
 - More Information:
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Appendix A – Agreement To Comply Form

Agreement to Comply With Information Security Policies

Employee Name (printed)

Department

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 these 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.

Employee Signature