

IMPORTANT INFORMATION

The following sample security policy is provided for your convenience only to assist you in developing a policy to address the security of cardholder information as required by the Payment Card Industry Data Security Standards (“PCI DSS”). NPC makes no representations that this sample security policy will satisfy your requirements under the PCI DSS as it relates to your environment. You may use the attached security policy as a template, but it is your responsibility to ensure that the security policy you implement meets all of your security needs.

In addition to complying with PCI DSS, you are also required to comply with all local, state and federal laws that apply to your business. One such law is the Fair and Accurate Credit Transactions Act (FACTA) that deals with the protection of cardholder data. **It is NPC’s policy that to be compliant with PCI DSS, a merchant must also be compliant with FACTA.**

FACTA is a federal law that states as follows: “no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any **receipt provided to the cardholder** at the point of sale or transaction.” 15 U.S.C. § 1681(c)(g).

It is every merchant’s responsibility to understand and comply with FACTA, and, in general, to protect the customer’s cardholder information. In addition, your business may be subject to other state laws that impact the information that you may print on receipts. It is a good business practice to regularly check the laws of your state to determine if you are compliant. You should evaluate your obligations under FACTA and all other applicable state laws and review your receipts to determine if the receipts are compliant with FACTA.

Additionally, effective December 31, 2010, all merchants will be required to truncate all but the last four digits of the customer’s cardholder number **on the merchant’s copy of electronically printed receipts**, and also mask the expiration date **on the merchants’ copy of electronically printed receipts**.

You should ensure that your security policy not only complies with the requirements of PCI DSS, but also complies with FACTA and all other applicable laws.

SAMPLE SECURITY POLICY

The Information Security Policy set forth by < Company Name > details the understanding and importance of sensitive data, especially that of cardholder data and the measures we will take to protect all such information.

Basic daily operational security procedures for the employees of < Company Name > include:

- Passwords must be < Company criteria > in length, expire within < # > of day, should not be written down or shared.
- All documents containing any element of cardholder data or customer bank account information will be maintained in a locked, secured fashion with limited access.
- The storage of CVV2 code or PIN data in any format / method is prohibited.
- Access to corporate systems and cardholder data information of < Company Name > will be given to employees based strictly on job function.
- Upon dismissal, an employee's access to all operations and data storage will be immediately revoked.

The same provisions apply if data is stored, processed, or transmitted through electronic means other than a stand-alone terminal (i.e. email, POS terminal connected to the internet, or gateway / shopping cart configuration). Usage of all peripherals and technologies storing, processing, or transmitting cardholder data require the following:

- Management approval
- A necessity for the technology
- Listing of all technologies, purposes for the technologies, and identification of personnel with access to such technologies
- Acceptable use of the technologies
- Automatic disconnect of modem session after a specific period of inactivity
- The inability to store cardholder data onto external media and the inability to cut and paste cardholder information.

Employees are to be made aware of < Company Name's > security policy and cardholder information practices upon hire and at least once a year thereafter. Employees will formally acknowledge the policy in writing.

If applicable, all third party service providers that <Company Name> uses to store, process, or transmit cardholder data on behalf of < Company Name > are PCI compliant and are contractually bound to secure cardholder data.

< Company Name > has an incident response plan, as set forth by PCI DSS requirements, in the event of a physical or electronic theft of cardholder data. The plan is tested annually.

Upon discovery of a cardholder breach, < Company Name > will immediately contact NPC Compliance at 1.800.376.3399, ext. 2737, or NPC Risk at 1.800.667.9624, to report the incident.

A designated Security Administrator has been assigned to ensure that the policy and the security practices of <Company Name> are enforced and updated, as needed.

