

PCI Compliance Policy

# Overview/Purpose

**<Utility Name>** is processing credit card payments for their Members; convenience. The PCI Security Standards Council, an organization established by the payment card industry, established Data Security Standard (DSS) which defines strict requirements for the processing, storage, and transmission of credit card data. **<Utility Name>** will meet these requirements by training employees and implementing appropriate policies and technology.

# Scope

PCI DSS requirements are addressed by many policies, procedures and standards of Information Security Program implemented by **<Utility Name>.** This policy addresses specific PCI DSS requirements only applicable to credit card payment processing.

# Policy

## Protect Stored Cardholder Data

### Prohibited Data

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted), beyond the life of the authorization transaction. Sensitive authentication data is defined as the following:

* The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. *(PCI Requirement 3.2.1)*
* The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance*. (PCI Requirement 3.2.2)*
* The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. *(PCI Requirement 3.2.3)*

No cardholder data of any type should be stored beyond that for which a legitimate business requirement exists. (*PCI Requirement 3.1)*

### Displaying PAN

**<Utility Name>** will mask the display of Primary Account Numbers (PANs) and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: *(PCI requirement 3.3)*

* A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access;
* PANs must be masked when displayed such that only personnel with a legitimate business need can see the full PAN;
* All other roles not specifically authorized to see the full PAN must only see masked PANs.

## Restrict Access to Cardholder Data by Business Need to Know

### Limit Access to Cardholder Data

* Access to **<Utility Name>** cardholder system components and data is limited to only those individuals whose jobs require such access. *(PCI Requirement 7.1)*
* Access limitations must include the following:
  + Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. *(PCI Requirement 7.1.2)*
  + Privileges must be assigned to individuals based on job classification and function (also called “role-based access control). *(PCI Requirement 7.1.3)*
  + *Query access to databases containing cardholder data must be restricted to authorized database administrators. (PCI Requirement 8.7)*

## Assign a Unique ID to Each Person with Computer Access

### Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the **<Utility Name>** network) to the network by employees, administrators, and third parties. *(PCI Requirement 8.3)* Remote access tokens or devices must be assigned to a specific account, and not used generically. (*PCI Requirement 8.6)*

### Access from Personal Devices

Any user-owned PCs or mobile devices used to access cardholder data must use personal firewall and anti-virus software acceptable to **<Utility Name>**. *(PCI Requirement 1.4)*

### Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. *(PCI Requirement 8.1.5)*

### User Accounts

For in-scope user accounts (those associated with the payment process), group, shared, or generic IDs, passwords must not be used. Additionally, the following authentication restrictions must be observed. *(PCI Requirement 8.5)*

* Generic user IDs are disabled or removed.
* Shared user IDs do not exist for system administration and other critical functions.
* Shared and generic user IDs are not used to administer any system components.

## Physically Secure All Areas and Media Containing Cardholder Data

* All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. *(PCI requirement 9.1.2)*
* Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:
  + All media must be physically secured. *(PCI requirement 9.5)*
  + Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. *(PCI Requirement 9.6)*
  + Media must be classified so the sensitivity of the data can be determined*. (PCI Requirement 9.6.1)*
  + Media must be sent by a secure carrier or other delivery method that can be accurately tracked. *(PCI Requirement 9.6.2)*
  + Management approval must be obtained prior to moving the media from the secured area. *(PCI Requirement 9.6.3)*
  + Strict control must be maintained over the storage and accessibility of media containing cardholder data. *(PCI Requirement 9.7)*

## Destruction of Data

Cardholder data for which a business need no longer exists will be deleted at least every 6 months.

All media containing cardholder data must be securely destroyed when no longer needed for business or legal reasons. *(PCI requirement 9.8)*

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. *(PCI requirement 9.8.1.a)*

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. *(PCI requirement 9.8.1.b)*

## Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted*. (PCI requirement 9.9)*

**<Utility Name>** must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: *(PCI requirement 9.9.1)*

* Make and model of all devices.
* Location of each device (for example, the address of the site or facility where the device is located).
* Device serial number or other method of unique identification.

The payment devices must be periodically inspected, including checks of surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *(PCI requirement 9.9.2)*

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: *(PCI requirement 9.9.3)*

* Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
* Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
* Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

## Service Providers

**<Utility Name>** shall implement and maintain policies and procedures to manage service providers. *(PCI requirement 12.8)*

This process must include the following:

* The maintaining of a list of service providers. *(PCI requirement 12.8.1)*
* The maintaining of a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. *(PCI requirement 12.8.2)*
* The implementation of a process to perform proper due diligence prior to engaging a service provider. *(PCI requirement 12.8.3)*
* The monitoring of service providers’ PCI DSS compliance status. *(PCI requirement 12.8.4)* The maintaining of information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity*. (PCI requirement 12.8.5)*

# Related Standards, Policies, and Processes

* PCI DSS Requirements   
  (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO** | **CFO CSR**  **HR** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |