Tender Care Animal Rescue

Tender Care Animal Rescue Information Security Policy

Overview
This policy is intended to help Tender Care Animal Rescue understand the importance of protecting cardholder data.

Purpose
To establish the Tender Care Animal Rescue's policy for the secure handling and transmission of sensitive card holder data including but not limited to magnetic strip data, PAN, expiration date, and service code.

Scope
This policy applies to all employees and systems of Tender Care Animal Rescue.

Technology Usage Policy

1.0 No unauthorized equipment can be brought into or set up in Tender Care Animal Rescue's facility. This includes, but is not limited to modems, computers, or wireless devices.

2.0 Wireless devices must be set up securely.

- 2.1 Do not use vendor default user accounts or passwords
- 2.2 Disable SSID broadcasts
- 2.3 Use the highest available encryption for the device

Incident Response Policy

1.0 Create and maintain procedures for handling security incidents.

- 1.1 All employees are to receive the incident response documents.
- 1.2 The incident response procedures are to be reviewed by all employees and updated annually.

Roles and Responsibilities

- 1.0 One or more Tender Care Animal Rescue employees will be designated with security responsibilities.

Cardholder Data Policy

- 1.0 Only Tender Care Animal Rescue employees with a business justification will have access to cardholder data.

2.0 All transmission of cardholder data over public lines must be encrypted.

2.1 All email transmissions containing PAN's must be encrypted.

3.0 Never store any of the following data types:

- Card verification codes or values
- Any track from the magnetic stripe
- Personal identification number (PIN)
- Encrypted PIN block

4.0 The PAN is to be masked, except where expressly allowed to be in full view.

5.0 All hardcopy and electronic cardholder data is to be identified and physically secured to ensure strict control over its accessibility.

5.1 Merchant – input how you secure these data type

- Computers(example, computers must stored be stored in a secure location)
- Electronic media(example, CD's are locked up when not in use)
- Networking and communications hardware(example, hardware is to be stored in a secure location)
- Telecommunication lines(example, RJ11 is located in a secure room)
- Paper receipts, reports, and faxes(example, receipts are stored in a locked drawer while not in use)

6.0 Distribution of media containing cardholder data either internally or externally must be strictly controlled.

6.1 Create and maintain procedures that ensure management approval is obtained prior to moving data from a secure location.

6.2 Data being transferred to external sources must be encrypted for electronic distribution. When the data is being transferred on physical media, for example a CD-ROM, it must be encrypted and a secure courier service must be used.

6.3 Any service provider that Tender Care Animal Rescue shares cardholder data with must adhere to the PCI DSS requirements, and acknowledge that they, the service provider, is responsible for the security for the cardholder data that they, the service provider, possess.

7.0 Cardholder data should not be retained any longer than is needed for justified business purposes or legal reasons. Once the data is no longer needed it should be securely destroyed.

7.1 Hard copy materials should be cross-cut shredded, incinerated, or pulped.
7.2 Electronic materials should be securely deleted

Review Policy

1.0 The PCI DSS policy is to be reviewed annually.

2.0 This policy is to be reviewed and updated annually to account for any changes in the Tender Care Animal Rescue environment and any changes in the PCI DSS requirements.