Credit Card Processing and Security Policy

The Wellbeing Farm

PURPOSE

The purpose of this policy is to define the guidelines for accepting and processing credit cards and storing personal cardholder information. The policy will help to ensure that cardholder information supplied to The Wellbeing Farm is secure and protected. The Wellbeing Farm is complying with credit card company requirements and the Payment Card Industry Data Security Standard.

DEFINITIONS

A. Payment Card Industry (PCI) Data Security Standard: THE PCI DSS is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly. To achieve compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

B. PCI:The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

C. Cardholder Data: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Cardmember ID (Discover) or CID - Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card.

D. System Administrator / Data Custodian: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of The Wellbeing Farm and/or third party vendors approved by the Managing Director may function as system/network administrators and/or data custodians.

SCOPE

This policy applies to all Wellbeing Farm employees. The policy pertains to all departments that process, transmit, or handle cardholder information. The cardholder information may be in a physical or an electronic format.

POLICY

All transactions that The Wellbeing Farm processes must meet the standards outlined in the policy.

A. Electronic credit card numbers should not be transmitted or stored on a personal computer or e-mail account. Electronic lists of customer's credit card numbers should not be retained. Credit card information should only be accepted online, by telephone, mail, or in person. This information should not be accepted via e-mail and departments should not e-mail credit card information.
B. Physical cardholder data must be locked in a secure area. Access should be limited to individuals that require the use of the data. Access should also be restricted on a 'need to know' basis.
C. Only essential information should be stored. Do not store the Card Verification Code (CVC). Do not store users PIN's or the full data from a cards magnetic stripe.
D. Credit card information should only be retained for the time needed to process, or if retained for reconciliation, for as long as one-year maximum if necessary.
E. Credit card information, if it does not need to be retained, should be destroyed. Information should be destroyed by shredding (cross-cut) immediately after processing, or immediately after they no longer need to be retained.
F. Credit card receipts may only show the up to the last five digits of the credit card number. If receipts show more than the last five digits, the receipts must be shredded or retained in a secure area.
G. All staff must comply with the Payment Card Industry Data Security Standard

https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

H. Exceptions to the policy may be granted by the Managing Director..

PROCEDURES

All credit card and debit card transaction acceptance, including web based transactions, must be initiated and controlled through the office.

Departments wishing to engage in electronic transactions are required to use The Wellbeing Farm's credit card processing system. Payment Sense is a safe and secure electronic payment mechanism. All servers and computers used for electronic transactions will be secure and Payment Card Industry compliant. Under no circumstance will it be permissible to obtain or send credit card information, or transmit credit card information by e-mail.

DATA STORAGE AND DESTRUCTION

The following processes must be followed for all data storage and destruction:

- Hardcopy containing cardholder data will be destroyed immediately after processing.
- All electronic media containing cardholder information should be labeled and identified as confidential.
- An inventory of media containing cardholder information should be performed monthly.
- Audit logs for system housing cardholder data will be available for a period of four (4) years.
- Electronic backup media containing cardholder data will be available for a period of four (4) years and then properly erased or decommissioned and destroyed on a monthly basis.

SANCTIONS

If the requirements of the policy are not followed, suspension of physical and/or electronic payment options will result. Fines may also be imposed by the affected credit card company.