HUNT Electric Corporation

ECSI System Integrators

POLICY TITLE: Customer and Employee Credit Card Security

ORIGINAL EFFECTIVE DATE: 03/2016

REVISION DATE:

PURPOSE

The Company is committed to protecting internal and external cardholder data necessary to conduct business.

POLICY

I. Credit Card Processing Systems
   A. Only authorized:
      1. Employees may use the Company's credit card processing systems.
      2. Employees of the Company may have access to cardholder data.
      3. Systems may be used for processing or storing cardholder data.

II. Cardholder Data
   A. Protecting Stored Cardholder Data
      1. Employees must adhere to the following requirements regarding non-storage of sensitive authentication data and cardholder data (even if encrypted):
         a. 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.
         b. 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.
         c. The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.
         d. The full credit card numbers are not stored under any circumstance.
   B. Transmitting Cardholder Data
      1. No cardholder data should be sent across open, public networks. This includes receiving or sending card information via email, text, IM or any other digital communications method.
   C. Sharing of Cardholder Data
      1. No cardholder data should be shared with any person or organization outside of the Company's authorized card processing employees and authorized card processing services.
   D. Restricting Access to Cardholder Data
      1. Access to the Company's cardholder system components and data is limited to only those individuals whose jobs require such access.
      2. Employees should not have access to cardholder data unless they are designated as a card processor or are giving a customer access to a card processor for purposes of exchanging needed information from the cardholder directly to the processor.
   E. Assigning a Unique ID
      1. All accounts used by credit card processors should be unique and not shared with any other person.

F. Restricting Physical Access to Cardholder Data
    1. No hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) should be stored.
    2. Any materials found with cardholder information should be destroyed.
    3. Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data.
    4. No cardholder data should be stored digitally in any our systems. This includes email, scanned images, accounting records or databases.

G. Destruction of Data
    1. All media containing cardholder data must be destroyed when no longer needed for business or legal reasons.
    2. Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents.

III. Breach or Loss

A. The department supervisor or CFO should be notified immediately of any suspected or real security incidents involving cardholder data:
    1. No one should communicate with anyone outside of their supervisor(s) or the CFO about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the supervisor or CFO.
    2. Document any information you know while waiting for the supervisor or CFO to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

B. The department supervisor or CFO should contact all affected parties in the event of a data loss or security breach event, which may include:
    1. Local authorities
    2. US Bank
    3. 3Delta - (703)234-6020
    4. Credit card providers (Visa, Mastercard, etc.)
    5. Credit card holder (customer)

I understand that it is my responsibility to read and comply with this policy and any revisions made to it. Please sign and date this policy and return to Human Resources.

_____ _____

Employee/Cardholder User's Signature Date

_____

Employee/Cardholder User's Name (Print)