DATA SECURITY POLICY

Policy Date: November 16, 2013
October 27, 2018
October 16 , 2021

Purpose:
CSCA makes use of credit card data from members and associates for several purposes. Receipt of this data may be electronic or paper. The purposes for receiving credit card data may include annual dues renewal, purchases of merchandise through CLumber CLoset, payments for goods and services associated with the National events, and other purposes.

CSCA values the security of credit card data and this policy is intended to ensure that the security of all credit card data received is maintained and that procedures are established with respect to the handling of this data.

Policy:

1. CSCA has an obligation to ensure that any credit card information received for any purpose is kept secure.
    a. The Treasurer has the responsibility of keeping a record of all transactions received using a credit card.
    b. Payments via Clumber Closet are processed by a third party service provider (WooCommerce) and credit card data is not stored by CSCA.
    c. Any third party service provider used by CSCA for web site credit card transactions via CLumber CLoset must employ data security protocols, such as SSL , SQL, or the equivalent, to ensure that transactions processed through the provider are secure.
    d. Upon a change in the Treasurer position, all user IDs, passwords and security questions used to gain access to credit card and other restricted and confidential data must be changed.
    e. The computer that is used to access systems that may store credit card or other confidential data must be protected by anti-virus software that is kept current. Virus scans should be run regularly.

    f. Firewalls should be in place and kept current to restrict access to computer systems that have access to credit card or other restricted confidential data.
    g. Only authorized CSCA members may access systems as is appropriate for their areas of responsibility, e.g. Treasurer, web site administrator, web site secretary, etc.
    h. Refunds for purchases will be made upon request made to the Clumber CLoset or the CSCA Treasurer. Refunds will be made for any item that is out of stock and no longer available. All other requests for refunds must state the reason for the refund and the Treasurer will determine if a refund is due and the amount. Any refunds due on purchases made via CLumber CLoset will be issued with a credit to the card used to make the original purchase.
2. Under no instance will Primary Account Number information be sent using email, text messaging, or any other unsecure messaging technologies.
3. All media used to send, receive or store credit card data must be kept secure.
    a. Computers used to send, receive, or store credit card data must be password protected.
    b. Access systems that store credit card data must be password protected and passwords changed periodically following the requirements of the service provider.
    c. All portable storage media must be password protected and/or encrypted.
    d. Portable devices used to access saved credit card data, such as smart phones, iPads, etc., must be password protected.
    e. Paper copies of credit card data must be kept in a secure area and destroyed once it is not needed.
4. All credit card data must be destroyed once its use it no longer needed.
    a. Electronic files must be deleted or rendered unrecoverable.
    b. Paper copies must be shredded, pulped, burned, or otherwise permanently destroyed.
    c. Any containers or storage devices holding information to be destroyed must be secured to prevent access to the information.
5. Any breach or misuse of credit card data will be dealt with as follows:
    a. The Treasurer will notify the President of CSCA of a breach via telephone or any other method to effect a quick notification.
    b. The person whose credit card information was breached will be notified by the Treasurer by telephone with a follow-up letter stating when the breach was noticed.
    c. Appropriate banking officials will be notified of the breach.
    d. Appropriate government officials will be notified of the breach.
    e. If necessary, legal counsel will be sought to oversee a breach occurrence.
6. Any service providers used to send or receive credit card data will be required to declare their ability to meet all federal data security regulations.
7. Annually the Treasurer will complete the PCI Security Questionnaire as required by the bank's merchant services department to assure compliance with federal regulations.
8. It is the responsibility of the CSCA Board to review this policy at least annually and to make any changes as may be necessary.