



Cottage Cove Credit Card Security Policy

Version 2 (Supersedes Version 1 dated Feb. 2009)

This document explains Cottage Cove's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program and our procedures to provide for securely processing financial transactions for our supporters who choose to utilize credit and debit cards.

In general, Cottage Cove staff is not permitted to transmit, process, or store credit card information on ministry or personal computer systems or through the Internet. When any donor to Cottage Cove visits a Cottage Cove website they must be directed to an approved and secure third party site to transmit, process, or store the credit card information.

Any unsolicited credit card information sent to the ministry via the internet shall not be acted upon apart from a secondary approved contact and the staff member is to advise the sender of the potential security risk of their previous contact. Cottage Cove will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Only personnel expressly authorized by the Executive Director are to have access to credit card information and only as needed to perform their job responsibilities. (PCI requirement 7.1) Apart from working with such data, all records are to be located in a secured environment. (PCI requirement 9.6) All hardcopy material containing cardholder data must be clearly marked as confidential (PCI requirement 9.7.1) and shall only be transferred outside of the facility by a secured courier or other delivery method that can be accurately tracked (PCI requirement 9.7.2). Materials may only be removed from their place of storage or designated workplace by prior authorization of the Executive Director. (PCI requirement 9.8)

Sensitive authorization data will be retained only until completion of the authorization of the transaction(s). All media containing cardholder data must be destroyed when no longer needed for business or legal reasons (PCI requirement 9.10) utilizing shredding, incineration or pulping (PCI requirement 9.10.1). Storage of sensitive authorization data post-authorization is forbidden. Specifically, sensitive authorization data includes the following:

- The full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. (PCI requirement 3.2.1)

- The card verification code or value (three- or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (PCI requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block. (PCI requirement 3.2.3)

All security incidents arising from the usage of credit card data must be reported to the Executive Director or his designate. Employees are not permitted to communicate with anyone outside of their direct supervisor, or the Executive Director, any details surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Executive Director or his designate, or a designate of the Board of Directors in the absence of the Executive Director.

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, files or paper records

Only the Executive Director, or Board of Directors, may establish a relationship with a service provider. The policies and procedures of this document will apply to all employees and any outside contractor involved with processing, storing or handling cardholder data. (PCI requirement 12.4) Any service provider must also maintain PCI DSS compliance. (PCI requirement 12.8.4)

Changes in circumstances require a mandatory review of this policy and related procedures. Otherwise, this policy is to be reviewed annually and shall automatically renew unless otherwise revoked or altered. (PCI requirement 12.1.1, 12.1.3)