Policy Direction – Handling Customer Credit Card Information

Rationale and Relationship to Mission, Principles and Values

The Multiple Sclerosis Society of Canada ("MS Society") is a national health charity that is highly dependent upon a variety of fundraising activities in order to carry out the mission of the organization. With over a million donors and 100,000 event participants annually supporting grassroots fundraising events such as MS WALK and MS BIKE and making donations online and via other means, there is a tremendous amount of highly sensitive credit card information that individuals employed or engaged by the MS Society must handle.

There are both legal and technical requirements that the MS Society must meet, in addition to our own organizational policies to protect the privacy and security of the information we steward. The MS Society's Privacy and Confidentiality Policy and related procedures are in place to ensure we meet our legislated requirements. In order to process credit card transactions, we are obligated to enforce technical standards via our contract with our financial institution which has adopted a set of standards referred to as the Payment Card Industry's Data Security Standard ("PCI-DSS").

There are both automated systems and manual processes in place for the handling of credit card information at the MS Society. Due to the importance of fundraising activities to raise the majority of our revenues, it is critical that the MS Society be PCI compliant in order that we can deliver on our mission. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised, all of which jeopardize our ability to deliver our mission and may harm the organization's credibility with the public.

Policy Objective

This policy direction is intended to describe the MS Society's proper handling of credit card transactions processed through automated systems and/or manual procedures. It provides a set of requirements to ensure that credit card information is handled and disposed of in a manner that satisfies the MS Society's obligation to protect such information to the level that meets or exceeds that required by the Payment Card Industry.

Since any unauthorized exposure of credit card information could subject the MS Society to reputational damage and significant penalties, failure to comply with this policy and related procedures will be considered a serious matter.

Policy Application

This policy applies to:

- Any individual who accepts, captures, stores, transmits and/or processes credit payments on behalf of the MS Society received for: the purchase of MS Society products and services, for registration to participate in MS Society fundraising events (e.g., MS Bike and MS Walk), contributions in the form of donations to the MS Society, or any other approved activity administered by the MS Society that would require the handling of credit card information.

- Any individual who supports any MS Society effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives him/her access to computer hardware and software holding credit card information, individuals tasked with shredding credit card information, and other individuals whose role would require handling of credit card information.

Authorization

The policy was approved by the MS Society of Canada Board of Directors on December 12, 2013.

Policy Details

The Executive Team is authorized to develop detailed procedures for this policy direction no later than six months following its approval.

1.0 Guiding Principles

1.1 PCI-DSS compliance is mandatory for all levels of the organization (national, divisional, and chapter) that accept, capture, store, transmit and/or process credit card information.

1.2 Training of individuals who handle customer credit card information is required no less than on a semi-annual basis. The contents of the training program must comply with the training requirements outlined in the detailed procedures for this policy direction.

1.3 Only authorized and properly trained individuals may accept and/or access credit or debit card information.

1.4 Credit card payments may be accepted only using methods approved by the MS Society national IT and Finance Departments.

1.5 Each person who has access to credit card information is responsible for protecting the information as per the MS Society Privacy and Confidentiality Policy.

1.6 Credit card information must be securely destroyed as soon as it has been processed as per the MS Society Privacy and Confidentiality Policy.

1.7 Departments must maintain appropriate checks and balances in the handling of credit card information.

1.8 Each department that handles credit card information must adhere to nationwide documented procedures from the national Finance Department in order to comply with this policy and PCI-DSS.

1.9 Suspected theft or loss of credit card information must be reported immediately to the National Vice-President, Shared Services, the Division President, and the appropriate national and/or divisional Privacy Officer.

Failure to comply with these principles, as implemented in this policy, may result in the revocation of the ability to process credit card transactions and/or could lead to disciplinary action, including termination of duties.

Executive Champion

The National Vice-President, Shared Services is the Executive Champion of this policy.

Monitoring and Compliance

The Executive Champion is responsible for ensuring that annual compliance audits are conducted, on a random basis, through trained internal resources and external third parties.

The Executive Champion and Division Presidents are responsible for reporting to the President and Chief Executive Officer through the quarterly compliance reports regarding compliance with this policy.

Related Policies, Legislation

- Payment Card Industry Security Standards Council; https://www.pcisecuritystandards.org
- MS Society Privacy and Confidentiality Policy and Procedures
- MS Society Information Technology Security Procedures
- MS Society Retention of Records Procedure

Policy Review

The policy is to be reviewed at least once every five years following approval.

____

Definitions:

Chapter - A subunit of a division and should be understood to mean the chapter office (if one exists), the chapter board and the activities that take place under the chapter name.

Division – The division head office, the division board, all chapters and other subunits that the MS Society board may create or delegate to be created from time-to-time and the activities that take place under the division name.

Executive Team – The most senior level of staff leadership within the MS Society comprised of the president and chief executive officer, division presidents, national vice-presidents of talent, research, marketing and development, programs and services, government relations, information technology, shared services. One person may hold more than one position. The president & chief executive officer may alter the composition of the Executive Team as required from time-to-time.

National office – The part of the MS Society that coordinates MS Society work as a whole, providing strategic oversight, and sharing of best practices in all functional areas. The National Office is responsible for administering the research program and direct marketing programs, for centralized financial processing, and management of a centralized information technology platform.

Payment Card Industry Data Security Standards (PCI-DSS) – To reduce their losses due to credit card fraud, members of the payment card industry came together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the PCI-DSS.