

## **Policy Direction – Handling Customer Credit Card Information**

### **Rationale and Relationship to Vision, Mission, and Values**

MS Canada 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. Annually hundreds of thousands of donors make donations online and via other means, towards MS Bike, MS Walk and We Challenge MS participants and teams. As such, there is a tremendous amount of highly sensitive credit card information that individuals employed or engaged by MS Canada must handle. All online donations are made securely through an encrypted server.

There are regulatory, legal and technical requirements that MS Canada must meet, in addition to our own organizational policies to protect the privacy and security of the information we steward. MS Canada'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 MS Canada. Due to the importance of fundraising activities to raise the majority of our revenues, it is critical that MS Canada 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 MS Canada'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 MS Canada'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 MS Canada 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 MS Canada received for: the purchase of MS Canada products and services, for registration to participate in MS Canada fundraising events (e.g., MS Bike and MS Walk), contributions in the form of donations to MS Canada, or any other approved activity administered by MS Canada that would require the handling of credit card information.
- Any individual who supports any MS Canada effort to accept, capture, store, transmit and/or process credit card information, such as a technical support staff member whose role gives them 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 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 MS Canada Corporate Services Department.
- 1.5 Each person who has access to credit card information is responsible for protecting the information as per MS Canada [Privacy and Confidentiality Policy](#).

2

<b>MS Canada – Policy Manual</b>	
<i>Applies to:</i>	All volunteers and staff at all levels
<i>Frequency of review:</i>	Annually
<i>First approved:</i>	December 12, 2013 by National Board of Directors
<i>Last reviewed:</i>	March 2021
<i>Next scheduled review:</i>	March 2022

- 1.6 Credit card information must be securely destroyed as soon as it has been processed as per MS Canada [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 VP Corporate Services, the VP, Community, the community senior director, and the 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 VP Corporate Services is the Executive Champion of this policy.

### **Monitoring and Compliance**

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

The VP Corporate Services and VP, Community are responsible for reporting to the President and Chief Executive Officer on a quarterly basis regarding compliance with this policy.

### **Related Policies, Legislation**

- Payment Card Industry Security Standards Council;  
<https://www.pcisecuritystandards.org>
- MS Canada [Privacy and Confidentiality Policy](#) and [Procedures](#)
- MS Canada [Information Technology Security Procedures](#)
- MS Canada [Retention of Records Procedure](#)

### **Policy Review**

The policy is to be reviewed at least once every year following approval as per PCI compliance requirements.

---

<b>MS Canada – Policy Manual</b>	
<i>Applies to:</i>	All volunteers and staff at all levels
<i>Frequency of review:</i>	Annually
<i>First approved:</i>	December 12, 2013 by National Board of Directors
<i>Last reviewed:</i>	March 2021
<i>Next scheduled review:</i>	March 2022

**Definitions:**

**Executive Team** – The most senior level of staff leadership within MS Canada comprised of the president and chief executive officer; division presidents; senior vice-president(s) and vice-president(s). One person may hold more than one position. The president and chief executive officer may alter the composition of the executive team as required from time-to-time.

**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.

<b>MS Canada – Policy Manual</b>	
<i>Applies to:</i>	All volunteers and staff at all levels
<i>Frequency of review:</i>	Annually
<i>First approved:</i>	December 12, 2013 by National Board of Directors
<i>Last reviewed:</i>	March 2021
<i>Next scheduled review:</i>	March 2022