YMCAs across Southwestern Ontario **POLICY**			
Function:	Governance	**Policy #:**	GV 3.12
Section:	Management	**Status:**	Published
Subject:	**Payment Card Industry Compliance**	**Status Date:**	2017-05-26
Issued to:	All Manual Holders	**Effective Date:**	2017-05-26
Approved by:	Chief Executive Officer	**Next Review Date:**	2018-04-26

1.0 POLICY

1.01 The Association shall protect the privacy of its customers and protect all credit card information entrusted to it to the fullest extent possible, including achieving and maintaining compliance with Payment Card Industry (PCI) requirements.

1.02 The Association must determine PCI-DSS requirement that are applicable based on the specific requirements outlined by PCI. This must be updated on an annual basis.

Credit Card Data Storage

1.03 Cardholder data should not be retained, either in paper or electronic formats longer than required to complete the payments transaction.

1.04 Cardholder card data that is stored in paper or electronic format must be rendered unreadable.

1.05 Sensitive Authentication data must not be stored in either paper or electronic form.

1.06 Immediately upon determination that a breach of credit card data has, or is suspected to have, occurred, the Risk Manager shall be notified and the Crisis Response protocol shall be initiated.

1.07 Immediately upon identifying a violation of a PCI standard, appropriate procedures are followed to mitigate the impact and the Risk Manager is notified.

PCI-DSS Controls

1.08 The Association must implement, and ensure functional effectiveness, for all the controls required by PCI-DSS, which may include policy, standard, process or technology controls.

1.09 Third-party contractors and vendors that process Cardholder card data must be PCI-compliant and provide confirmation of this compliance to the Association at least annually.

1.10 The Association must test the controls identified in 1.01 and confirm that they are operating effectively on an annual basis.

1.11 Internal and external penetration tests must be performed on any cardholder data environment, as required by PCI on a quarterly basis. External penetration tests must be performed by an Approved Scanning Vendor (ASV).

Self-Assessment Questionnaire Completion

1.12 The Association must complete and sign an SAQ on an annual basis. The SAQ type is to be determined based upon the requirements identified by PCI and the Merchant.

1.13 The completed and signed SAQ, along with any ASV reports, must be provided to each Merchant used by YMCA to process credit card payments, on an annual basis.

1.14 The completed and signed SAQ must be retained in compliance with IT 5.06 Record Retention Policy, along with all documentation of PCI-DSS Controls testing and ASV scanning result

1.15 All users are strictly required to comply with the statements established in this YMCA PCI Compliance Policy. Non-compliance may result in disciplinary action up to and including termination of employment.

1.16 Any exceptions must be formally and thoroughly documented and addressed directly to the policy approver.

1.17 All queries related to the PCI Compliance Policy should be directed to the Chief Financial Officer.

2.0 PURPOSE

2.01 The purpose of this policy is to demonstrate compliance with PCI requirements.

2.02 The purpose of this policy is to prescribe a comprehensive framework for protecting credit data and related information systems.

3.0 SCOPE

3.01 This policy applies to all YMCA internal and external employees, as well as third party contractors, volunteers and vendors with access to credit card data (also known as cardholder data).

4.0 RESPONSIBILITY

4.01 All employees, contractors, volunteers and third party personnel with access to the Association credit card data and information systems that hold this data are responsible for adhering to the statements detailed in this policy. Managers and Supervisors are responsible for ensuring adherence to policy guidelines.

4.02 The Chief Financial Officer will own this policy and be responsible for ensuring its applicability and compliance. This includes reviewing the results of all testing of PCI-DSS controls and signing the annual SAQ.

4.03 Managers and Supervisors and the Executive Management Team will review and provide update commentary to this policy, annually to address any changes in the Association environment.

5.0 DEFINITIONS

5.01 **Cardholder Data Environment (CDE)** – Includes the people, processes and technologies that store, process, or transmit credit card data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

5.02 **Cardholder Data** – As defined by PCI, Cardholder data includes the Primary Account Number (PAN), Cardholder Name, Expiration Date and Service Code.

5.03 **Merchant** - is a person whose job is to buy and sell products in large amounts.

5.04 **Must** means not optional. Adherence to the policy statement is mandatory.

5.05 **Payment Card Industry** (PCI) standards mean the set of standards created by the payment card industry to reduce their losses due to credit card fraud. Additional information is available at https://www.pcisecuritystandards.org.

5.06 **PCI-DSS** means Payment Card Industry – Data Security Standard.

5.07 **PIN** – Personal identification number.

5.08 **Self-Assessment Questionnaire (SAQ)** - Reporting tool used to document self-assessment results from the YMCA's PCI-DSS assessment.

5.09 **Sensitive Authentication Data** – as defined by PCI, sensitive authentication data includes magnetic strip data or equivalent on a CHIP/PIN card, Card Validation Value or Code (CVV) and PIN numbers.

5.10 **Should** means optional. Adherence to the policy statement is preferred but not mandatory.

6.0 REFERENCES AND RELATED STATEMENTS OF POLICY

Type	Reference
Law, regulation, governing document	Payment Card Industry (PCI)Standards *Personal Information Protection and Electronic Documents Act (PIPEDA)*
Other external reference	*Centre for Internet Security (CIS)* *International Organization for Standardization (ISO)* *SysAdmin Audit Network Security (SANS) Institute* *National Institute of Standards Technology (NIST). Control Objectives for Information and Related Technology (COBIT)* *Information Technology and Control Guidelines (ITCG)*
Policy	FN 1.05 Credit and Debit Card Payments IT 8.04 Confidentiality and Privacy IT 9.06 Data Encryption GV 1.12 Protecting Children and Vulnerable Persons GV 1.10 Ethics and Business Conduct
Process	01-08-002 PCI Compliance Application

7.0 APPLICATION

08-06-002 PCI Compliance Application

8.0 ATTACHMENTS

None

Review & Approval Record

This policy is to be reviewed at least:

Document all reviews here prior to updating Next Review Date for a Policy

Date	Reviewed by	Approved by
2017-05-05	IT Manager	
2017-05-26	Chief Financial Officer	

Revision Control

Document all revisions here prior to issuing an updated Policy

Date	Revision
2013-10-01	Drafted Policy Document
2017-04-13	Update policy issued. PCI Standards included.