Credit Card Policy and Procedures

I. PURPOSE

The purpose of this policy is to establish business processes and procedures for accepting Credit and Debit cards at Personal Image and Massage Inc that will minimize risk and provide the greatest value, security of data, and availability of services to each PERSONAL IMAGE AND MASSAGE INC. Member within the rules and regulations established by the Payment Card Industry (PCI) and articulated in the PCI Data Security Standards (DSS). Additionally, these processes are intended to ensure that payment card acceptance procedures are appropriately integrated with the PERSONAL IMAGE AND MASSAGE INC.’s accounting and other systems.

II. BACKGROUND

In response to increasing incidents of identity theft, the major payment card companies created the Payment Card Industry Data Security Standard (PCI DSS) to help prevent theft of customer data. PCI DSS applies to all businesses that accept payment cards to procure goods or services. Compliance with this Standard is enforced by the payment card companies and generally, noncompliance is discovered when an organization experiences a security breach that includes cardholder data.

Security breaches can result in serious consequences for PERSONAL IMAGE AND MASSAGE INC., including release of confidential information, damage to reputation, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept payment card and eCommerce payments. PERSONAL IMAGE AND MASSAGE INC. will take every effort to ensure that Data Security Standards are adhered to.

III. DEFINITIONS

Cardholder

The customer to whom a credit or debit card has been issued or the individual authorized to use the card

Cardholder Data

All personally identifiable data about the cardholder (i.e., account number, expiration date, and cardholder name.)

PERSONAL IMAGE AND MASSAGE INC. Management

Executive officer that approves all third-party service providers and coordinates the policies and procedures for accepting Credit and Debit cards at PERSONAL IMAGE AND MASSAGE INC.

Encryption

The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.

Staff Employee

For the purposes of the PCI DSS and this policy, a Staff Employee is defined as entity that accepts Credit or Debit cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or VISA) as payment for PERSONAL IMAGE AND MASSAGE INC. training and/or services.

PERSONAL IMAGE AND MASSAGE INC. Accounting

Accounting and non-exempt employee within a department who has primary authority and responsibility for Credit or Debit card and eCommerce transaction processing within that department.

Payment Card

Any Credit or Debit card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.

Credit or Debit Card Account Change

Any change in the payment account including, but not limited to:

* the use of existing Credit or Debit card accounts for new purposes
* the alternation of business processes that involve Credit or Debit card processing activities;
* the addition or alteration of payment systems;
* the addition or alternation of relationships with third-party Credit or Debit card service providers, and
* the addition or alternation of Credit or Debit card processing technologies or channel

Credit or Debit Card Industry (PCI) Data Security Standard (DSS)

A multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Sensitive Authentication Data

Security-related information (card validation codes/values, full magnetic-stripe data, or personal identification number (PIN)) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form

IV. TERMS AND CONDITIONS

This policy applies to all PERSONAL IMAGE AND MASSAGE INC. employees, Members, Non-Members, Consultants, or Agents who, in the course of doing business on behalf or with PERSONAL IMAGE AND MASSAGE INC., accept, process, transmit, or otherwise handle cardholder information in physical or electronic format.

This policy applies to all PERSONAL IMAGE AND MASSAGE INC. departments and administrative areas which accept Credit or Debit cards regardless of whether revenue is deposited in a PERSONAL IMAGE AND MASSAGE INC. financial account.

V. ACCEPTABLE CREDIT OR DEBIT CARDS

PERSONAL IMAGE AND MASSAGE INC. currently accepts VISA, MasterCard, Discover and American Express Card and has negotiated contracts for processing Credit or Debit card transactions. Individual PERSONAL IMAGE AND MASSAGE INC. employees may not use or negotiate individual contracts with these or other Credit or Debit card companies or processors. All individual PERSONAL IMAGE AND MASSAGE INC. employees must use the PERSONAL IMAGE AND MASSAGE INC. negotiated contract.

VI. PROHIBITED CREDIT OR DEBIT CARD ACTIVITIES

PERSONAL IMAGE AND MASSAGE INC. prohibits certain credit card activities that include, but are not limited to:

* accepting Credit or Debit cards for cash advances
* discounting training or service based on the method of payment
* adding a surcharge or additional fee to Credit or Debit card transactions

VII. CREDIT OR DEBIT CARD FEES

Each Credit or Debit card transaction will have an associated fee charged by the credit card company.

PVIII. REFUNDS

When a service is purchased using a Credit or Debit card and a refund is necessary, the refund must be credited back to the account that was originally charged. Refunds in excess of the original sale amount or cash refunds are prohibited

IX. CHARGEBACKS

Occasionally a customer will dispute a Credit or Debit card transaction, ultimately leading to a chargeback. In the case of a chargeback, PERSONAL IMAGE AND MASSAGE INC.’s accounting department will be responsible for all chargeback transactions.

X. MAINTAINING SECURITY

Departments and administrative areas accepting Credit or Debit cards on behalf of PERSONAL IMAGE AND MASSAGE INC. are subject to the Credit or Debit Card Industry Data Security Standards (PCI DSS).

Fax transmissions (both sending and receiving) of credit card and electronic payment information occurs using only fax machines which are attended by those individuals who must have contact with Credit or Debit card data to do their jobs;

PERSONAL IMAGE AND MASSAGE INC. requires that all external services providers that handle Credit or Debit card information be PCI compliant.

PERSONAL IMAGE AND MASSAGE INC. restricts access to cardholder data to those with a business “need to know.”

For electronic media, cardholder data shall not be stored on servers, local hard drives, or external (removable) media including floppy discs, CDs or thumb (flash) drives unless encrypted and otherwise in full compliance with PCI DSS.

For paper media, cardholder data shall not be stored.

XI. RESPONSIBILITIES

PERSONAL IMAGE AND MASSAGE INC. Staff are responsible for:

Executing on behalf of the relevant PERSONAL IMAGE AND MASSAGE INC. Department, Credit or Debit Card Account Acquisition or Change Procedures.

Ensuring that all employees, contractors and agents with access to Credit or Debit card data within the relative PERSONAL IMAGE AND MASSAGE INC. Department acknowledge on an annual basis and in writing that they have read and understood this Policy. These acknowledgements should be submitted, as requested, to PERSONAL IMAGE AND MASSAGE INC.’s accounting department

Ensuring that all Credit or Debit card data collected by the PERSONAL IMAGE AND MASSAGE INC. Department in the course of performing PERSONAL IMAGE AND MASSAGE INC.’S business, regardless of whether the data is stored physically or electronically is secured. Data is considered to be secured only if all of the following criteria are met:

Only those with a "need-to-know" are granted access to Credit or Debit card and electronic payment data;

Email should not be used to transmit credit card or personal payment information. If it should be necessary to transmit credit card information via email only the last four digits of the credit card number can be displayed;

Credit card or personal information is never downloaded onto any portable devices or media such as USB flash drives, compact disks, laptop computers or personal digital assistants;

The processing and storage of personally identifiable credit card or payment information on PERSONAL IMAGE AND MASSAGE INC. computers and servers is prohibited;

Only secure communication protocols and/or encrypted connections to the authorized vendor are used during the processing of eCommerce transactions

The three- or four-digit validation code printed on the Credit or Debit card is never stored in any form;

The full contents of any track data from the magnetic stripe are never stored in any form

The personal identification number (PIN) or encrypted PIN block are never stored in any form;

The primary account number (PAN) is rendered unreadable anywhere it is stored;

All but the last four digits of any credit card account number are masked when it is necessary to display credit card data;

All media containing Credit or Debit card or personal payment data is retained no longer than a maximum of six (6) months and then destroyed or rendered unreadable; and

Notifying the Executive Director, Accounting Manager in the event of suspected or confirmed loss of cardholder data. Details of any suspected or confirmed breach should not be disclosed in any email correspondence. After normal business hours, notification shall be made to the Executive Director.

A PCI compliant company shall regularly monitor and test the PERSONAL IMAGE AND MASSAGE INC. Network and coordinate PERSONAL IMAGE AND MASSAGE INC.’s compliance with the PCI Standard’s technical requirements and verify the security controls of systems authorized to process credit cards.

PERSONAL IMAGE AND MASSAGE INC. will conduct Internal Auditing to:

Periodically will review PERSONAL IMAGE AND MASSAGE INC. employee compliance with this policy and the Credit or Debit Card Industry (PCI) Data Security Standards (DSS);

Identify unapproved payment applications or external vendors that collect Credit or Debit card data on behalf of the PERSONAL IMAGE AND MASSAGE INC. and notify Accounting Department; and

When required will conduct the PERSONAL IMAGE AND MASSAGE INC.’s PCI DSS Self-Assessment and complete the PERSONAL IMAGE AND MASSAGE INC.’s Attestation of Compliance