POLICY:		Credit Card Security Policy

FIRST DRAFT:		22.05.14

ADOPTED:		BR 2014#02 pro-tem1 BR 2014#04

AMENDMENTS:		None to Date

REVIEW:		June 2019

[1] Pending consultation in accordance with the Protocol for Policy Development

Mary Immaculate College

Credit Card Security Policy

PCI DSS 2.0

22/05/2014

Introduction and Scope

All policies, guidelines and protocols of Mary Immaculate College, will reflect the Colleges commitment to the promotion of equality and will be fully compliant with the provisions of prevailing equality legislation.

Introduction

This document explains Mary Immaculate College's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Mary Immaculate College management is committed to this security policy to protect information utilized by Mary Immaculate College in attaining its business goals. All employees are required to adhere to the contents described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Mary Immaculate College's cardholder environment consists only of imprint machines or standalone dial-out terminals. The environment does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) B, ver. 2.0, October, 2010. Should Mary Immaculate College implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ B, it will be the responsibility of Mary Immaculate College to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable.

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):
The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance.
The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance.
The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

Displaying PAN

Mary Immaculate College 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.

Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

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

Restrict Access to Cardholder Data byBusiness Need to Know

Limit Access to Cardholder Data

Access to Mary Immaculate College's cardholder system components and data is limited to only those individuals whose jobs require such access.

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control).

Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured.

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

Media must be classified so the sensitivity of the data can be determined.

Media must be sent by a secure carrier or other delivery method that can be accurately tracked.

Logs must be maintained to track all media that is moved from a secured area, and management approval must be obtained prior to moving the media.

Strict control must be maintained over the storage and accessibility of media containing cardholder data.

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons.

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents.

Security Incident Response

Incident Identification

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, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records

Reporting an Incident

The Data Compliance Office should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the Data Compliance Office to report any suspected or actual incidents. The Security Office phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Data Compliance Office about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Data Compliance Office.

Document any information you know while waiting for the Data Compliance

Office to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.
2. Alert all necessary parties. Be sure to notify:
   a) Merchant bank
   b) Authorities (if appropriate)

3. Perform an analysis of legal requirements for reporting compromises where clients were affected.

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Data Compliance Office will work with legal and management to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Data Compliance Office and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their

appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

Mary Immaculate College shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security.

Service Providers

Mary Immaculate College shall implement and maintain policies and procedures to manage service providers.

This process must include the following:

- Maintain a list of service providers
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess Implement a process to perform proper due diligence prior to engaging a service provider
- Monitor service providers' PCI DSS compliance status