McMaster Payment Card Industry Data Security Standards (PCI-DSS) Steering Committee

TERMS OF REFERENCE

1. Objectives

1. To ensure that the University complies with Payment Card Industry Data Security Standards (PCI-DSS) thus allowing the University to continue to process payment cards and eCommerce.
2. To minimize reputational risks and legal liabilities associated with leakage of customer payment card and eCommerce information
3. To oversee the University's response to any identified known or potential breach of customers' payment card and eCommerce data.
4. Provide guidance to Departments on Payment Card and eCommerce Processing Best Practices.

2. Accountability

1. Develop and recommend to President and Vice Presidents (PVP), policies and procedural guidelines pertaining to the management of customers' Payment (Credit and Debit) card and eCommerce information at the University and ensure compliance with these policies and procedures.
2. Develop minimum standards for University payment card and eCommerce merchants and monitor compliance with standards.
3. Review the results of the Annual Payment Card Compliance Attestation Process and Action Plans for non-compliant merchants, and take steps to have merchants not in compliance with procedures to reach compliance, or if not possible recommend other actions (including suspension of merchant account)
4. Review reports from UTS, Finance, and Internal Audit with respect to department compliance with standards.
5. Develop, maintain and promote standard operating procedures for response to potential security breaches.
6. Oversee and coordinate the University response to any suspected PCI-DSS related data incidents (possible security breaches) through UTS IT Security.
7. Initiate and oversee projects to improve the security or service levels for payment card and eCommerce transactions across the University.
8. Review requests for new payment card and alternative ecommerce payment merchants
9. Monitor Chargebacks and recommend appropriate systematic changes that may reduce these, as appropriate.
10. Oversee progress of merchants to new requirements as implemented.
11. Resolve issues relating to payment card and ecommerce processing as they arise.
12. Act as a forum to keep communications open between the various administrators involved with payment processing.
13. Sponsor workshops to ensure all parties are up to date and knowledgeable of applicable policies and procedures
14. Maintain overall responsibility for compliance to Payment Card Industry standards and with the University Preferred Payment Provider Contract and Approved Alternate Payment Provider

3. Request for Exceptions

1. The Co-Chairs (CTO and CFO) of the PCI-DSS Steering Committee, on recommendation of the PCI-DSS Steering Committee, have the authority to grant exceptions to the *"Policy for Acceptance of Payments Cards and eCommerce"*

4. Meetings

1. The CFO is responsible for setting the annual meeting schedule for the PCI-DSS Steering Committee and for preparing or coordinating reports to be presented to the PVP as required.
2. PCI-DSS Steering Committee will meet quarterly, or on a schedule as amended by the Committee. Additional meetings may be called at the discretion of either Co-Chair.
3. Quorum consists of at least six (6) members of the Committee provided that one of the six (6) is one of the Co-Chairs
4. Members may attend meetings in person or by conference call or other electronic methods. Members may opt to "add delegates" pin situations when they are unable to attend a meeting.

5. Membership

- AVP Administration and CFO – Co-Chair
- Assistant Vice President & Chief Technology Officer – Co-Chair
- Controller, FA
- Director, Information Security, UTS
- Information Systems Manager, Housing and Conference Services, CSU
- Technology Manager, Applications Development, CSU
- Manager, Financial Reporting, FA
- Director, Alumni Advancement, UA
- Manager, Student Accounts and Cashiers
- Manager, Information Systems, Hospitality Services
- Manager of Finance and Administration, CCE
- Information Security Officer, UTS
- Manager, Finance and Administration, A&R
- Manager Internal Auditor, Audit and Risk Services (ex-officio)

6. Approval

Original approval – October 2008,
Updated – November 2011, March 2016, February 2018, October 2018, October 2019, April 2020, January 2021.