PCI Information Security Policy

Document Details

Document Reference/Name:
PCI Information Security Policy

Version Number:
1.00

Documentation Status:
☒ Working Draft ☐ Published ☐ Approved ☐ Adopted

Domain:
PCI Information Security

Last Review Date:
03/26/2014

Document Owner:
City of Minneapolis Finance Department

Version History:

Version Number	Date	Reason/Comments
1.00	November, 2013	Document Origination

PCI Information Security Policy

I. Purpose

This document has been created for adoption by the City Council of Minneapolis to ensure compliance with the Payment Card Industry Data Security Standard ("PCI DSS"). The data that resides at and is transmitted from the City of Minneapolis merchant locations includes cardholder data as defined by the Payment Card Industry Security Standards Council. Due to the value of cardholder data and contractual requirements of processing credit cards it is a high priority for the City of Minneapolis to protect such data and maintain compliance with the Payment Card Industry Data Security Standard.

II. Scope

This policy applies to all City of Minneapolis departments served by the Finance Department that process, transmit or store cardholder data in any tangible manner.

III. Definitions

Cardholder data environment – The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.

Risk Assessment - Process that systematically identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

Acquiring Bank - Also referred to as "merchant bank," or "acquiring financial institution." The entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

Payment Brand - The five global payment brands include: American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

IV. Policy

The City of Minneapolis will protect cardholder data that is processed, transmitted, or stored within any City of Minneapolis cardholder data environment in compliance with the Payment Card Industry Data Security Standard.

Any City of Minneapolis department found to have violated this policy may be subject to sanctions up to and including removal of authorization to process credit card transactions.

V. Roles and Responsibilities

Chief Finance Officer and/or those delegated by the Chief Finance Officer will:

- Establish, publish, maintain, disseminate and annually review procedures for the ongoing maintenance of this policy, that:

  - Ensure all departments that perform credit card transactions within the City of Minneapolis maintain and adopt department level procedures, standards, and/or guidelines that address all applicable PCI DSS requirements;
  - Ensure all departments, as required by PCI DSS, conduct an annual formal risk assessment of threats and vulnerabilities related to their cardholder data environment;
- Authorize credit card processing for all departments that have complied with the PCI DSS requirements; and
- Submit the annual PCI DSS Attestation of Compliance to the acquiring bank, PCI Security Standards Council, and/or payment brands as required.