CITY OF SPOKANE
ADMINISTRATIVE POLICY

ADMIN 5600-19-08
LGL 2017-0031

TITLE: PCI COMPLIANCE
EFFECTIVE DATE: JULY 14, 2017
REVISION EFFECTIVE DATE: JANUARY 25, 2019

1.0 GENERAL

1.1 This policy establishes guidelines for information security standards, including the Payment Card Industry Data Security Standards (PCI-DSS), which is a set of comprehensive requirements for enhancing payment security. PCI-DSS was by the founding payment brands of the Payment Card Industry Security Standards Council (PCI-SSC). The PCI-SSC is responsible for managing the security requirements, while the founding members of the Council enforce compliance with the PCI set of standards: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

1.2 PCI-DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent primary account number (PAN) card fraud, hacking and various other security vulnerabilities and threats.

1.3 The standards are to protect cardholder information on behalf of any individual or entity that use a PAN to transact business with the City of Spokane. This policy is in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

1.4 TABLE OF CONTENTS

2.0 DEPARTMENTS/DIVISIONS AFFECTED

2.1 Applicable to all departments who have access to PAN card information, including:

2.1.1 Every employee that accesses, handles, or maintains PAN card information. The City of Spokane employees include full-time, part-time and hourly staff members as well as intern and student workers who access, handle, or maintain records.

2.1.2 Employees who contract with service providers (third-party vendors) who process PAN payments on behalf of the City of Spokane.

2.1.3 Employees who manage events and require payment-processing capabilities (e.g. PayPal).

2.1.4 Category 1 Entities: All departments that collect maintain or have access to PAN card information.

2.1.5 Category 2 Entities: All departments managing or utilizing a hosted payment gateway or any other online payment service to collect payments through an access point that is PCI compliant by the City of Spokane, even though these entities do not have access to PAN card information.

2.1.6 Category 3 Entities: All departments who have relationships with third-party vendors that serve as access points through PayPal, or any other payment services.

2.1.7 Third-party vendors that process and/or store PAN card information on behalf of the City of Spokane and using the city's merchant identification number (MID) accounts.

3.0 REFERENCES

City of Spokane's Information Security Policy - ADMIN 5300-17-06

National Institute of Standards and Technology (NIST) Cybersecurity Framework Guideline - Version 1.1

Payment Card Industry Data Security Standard (PCI-DSS) Version 3.2.1- Sections: 12.4 and 12.8

RCW 19.255.020 Liability of Processor, businesses, and vendors

RCW 42.56.420 Security

4.0 DEFINITIONS

4.1 “Cardholder Data Environment (CDE)” is the approved electronic payment and authentication systems supported by the Innovation and Technology Services Department (ITSD).

4.2 “MID” is the Merchant Identification Number which is a relationship set up between the COS and Elavon, the City’s third-party processor to track certain lines of business or certain PAN activity. The MID is tied to a bank account for the settlement of the credit card transactions.

4.3 “PAN” is an individual’s primary account number. The PAN is the payment card number that identifies the issuer and the particular cardholder account.

4.4 “PCI Compliance Coordinator” which is defined by the Information Security Officer (ISO), is someone who is responsible for compliance in consultation with the Director of Accounting, will be responsible for staying abreast of changes to PCI-DSS requirements.

4.5 “PCI Department Contact” is the representative within Category 1 departments who are responsible for ensuring that their department has policies and procedures in place to comply with PCI and data security requirements.

4.6 “PCI-DSS” is the Payment Card Industry Data Security Standard. PCI-DSS is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

4.7 “PCI Security Standards Council” is the security standards council that defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

4.8 “Self-Assessment” is the PCI Self-Assessment Questionnaire (SAQ). SAQ is a validation tool that demonstrates compliance to the PCI DSS.

4.9 “PAN Card Data” is the full magnetic stripe or the PAN (Primary Account Number) plus any of the following: Cardholder name, Expiration date and the Service Code

5.0 POLICY

5.1 The City of Spokane shall adhere to the PCI-DSS Version 3.2.1 Requirements of the PCI-SSC.

5.2 City of Spokane prohibits the storage of any PAN card information in an electronic format on any computer, server or database.

5.3 All employees within Categories 1, 2 and 3 must read, understand and agree to adhere to this policy and any other Information Security policies of the City of Spokane.

5.3.1 Without adherence to the PCI-DSS standards, the City of Spokane would be in a position of unnecessary reputational risk and financial liability. If the City of Spokane failed to comply the city would be subject to:

a. Any fines imposed by the payment card industry.

b. Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees.

c. Suspension of the MID account.

5.4 General Requirements:

5.4.1 The Director of Accounting shall approve credit card MID's.

5.4.2 Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data shall be brought to the attention of the Director of Accounting and the PCI Compliance Coordinator.

5.4.3 A list of card processing terminals are to be maintained and updated when change occurs.

5.5 Category 1 Requirements (in addition to the general requirements above):

5.5.1 Management in departments accepting/processing credit cards must correlate with the PCI Compliance Coordinator for the competition of an annual self-assessment.

5.5.2 The PCI Department Contact must create or confirm the existence of appropriate policies and procedures for credit card processes, storage, and destruction of card data.

5.5.3 Access to the cardholder data environment must be restricted to only those employees with a need to access such environments and physical controls must be in place to protect the cardholder data environment.

5.5.4 Periodic inspections of device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) shall be required.

5.6 Category 2 Requirements (in addition to the general requirements above):

5.6.1 Management in Category 2 departments using PayPal or other Director of Accounting approved online payment services for event or service payments must ensure that all personnel within their department understand the City of Spokane policies on accepting PAN.

5.6.2 Employees managing/sponsoring events or services for which PayPal or other Director of Accounting approved online payment services are used must confirm knowledge of and adherence to the above policy when requesting PayPal or other approved online payment service access/mailbox from the Director of Accounting.

5.7 Category 3 Requirements (in addition to general requirements above);

5.7.1 Management in Category 3 departments must confirm that the third-party vendors through whom they are accessing PayPal or other services are reviewed and approved by the Director of Accounting and the ISO.

5.8 Storage and Disposal

5.8.1 Credit card information shall not be stored on any electronic device, including City of Spokane network servers, workstations, laptops, tablets and cellular phones.

5.8.2 Credit card numbers shall never be sent via electronic mail including but not limited to, email (SMTP), skype messaging, voicemail, fax, text messaging or any other method that may store or transmit electronically

5.8.3 Neither the full contents of any track of the magnetic stripe nor the three-digit card validation code may be stored in a database, log file, electronic document or point of sale product.

5.8.4 Programming all credit card processing machines so that the printout only the last four or first six characters of a credit card number.

5.8.5 Destruction of sensitive cardholder data is required when no longer needed for reconciliation, business or legal purposes is required. Secured destruction must be via crosscut shredding in house or with a third-party provider with certificate of disposal.

5.9 Third-Party Vendors (Processors, Software Providers, Payment Gateways, or other Service Providers)

5.9.1 In coordination with the PCI Compliance Coordinator, before a final decision is made, the Director of Accounting shall approve the following scenarios:

a. Any merchant bank or processing contract of any third-party vendor that is engaged in, or proposes to engage in, the processing or storage of transaction data on behalf of City of Spokane—regardless of the manner or duration of such activities.

b. Ensuring that all third-party vendors adhere to all rules and regulations governing cardholder information security.

c. Ensuring contract requirements are met from all third parties that are involved in credit card transactions meet all PCI security standards, and that they provide evidence of compliance and their efforts at maintaining ongoing compliance.

5.10 Encryption

5.10.1 All transmissions of credit card data must use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, ensuring that, only trusted keys and certificates are accepted, the protocol in use only supports secure versions or configurations, and the encryption strength is appropriate for the encryption methodology in use.

5.11 Additional Requirements

5.11.1 Web payments must be processed using a PCI-compliant service provider approved by the Director of Accounting.

5.11.2 Although electronic storage of credit card data is prohibited by this policy, the City of Spokane will perform a quarterly network scan both internally and externally against the cardholder data environments to ensure that the policy has not been violated.

5.12 Training

5.12.1 New and existing employees that interact with payment cards must undergo PCI training at the point of hire and annually.

6.0 RESPONSIBILITIES

6.1 Self-Assessment

6.1.1 The PCI Compliance Coordinator shall complete the PCI-DSS Self-Assessment Questionnaire annually and anytime a credit card related system or process changes.

6.1.2 ITSD staff shall be responsible for ensuring no PAN card information is stored electronically.

6.2 Responsible Organization/Party

6.2.1 The Director of Accounting shall administer this policy, which includes responsibility for notifying the ISO, applicable Department Heads and Data Managers about changes to the policy.

6.2.2 The Director of Accounting shall approve all departments hosting/sponsoring activities/conferences/programs with payments through PayPal or any other payment gateway.

6.3 Enforcement

6.3.1 With the assistance of the Director of Accounting, the ISO will oversee enforcement of the policy. Additionally this individual will investigate any reported violations of this policy, coordinate investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy.

6.3.2 The PCI Department Contact shall enforce the following list:

a. Ensure that all departmental personnel with access to PAN card data receive appropriate training and are knowledgeable about this policy.

b. Suggest updates to this policy, and serve as point of contact for PCI department contacts with regard to assessment surveys or other PCI issues.

7.0 APPENDICES

7.1 PCI DSS Quick Reference Guide Version

APPROVED BY:

1/9/2019

Eric Finch
Chief Innovation and Technology Officer

Date

Michelle Hughes 12/04/18

Michelle Hughes
Director of Accounting

Date

Theresa Sanders 1/10/19

Theresa Sanders
City Administrator

Date

James 12/04/18

James Richman
City Assistant Attorney

Date