BTS-2.17 - Payment Card Security Standards

PAYMENT CARD SECURITY STANDARDS
Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority
ARB-BTS-2.17

Purpose

The City collects payments using payment cards (credit and debit cards) for a variety of purposes. The payment cardholder association (Visa, Mastercard, American Express) requires that the City abide by specific information security standards, known as Payment Card Industry- Data Security Standards (PCI-DSS) in order to be permitted to process electronic payments using various payment cards.

This section outlines specific PCI-DSS requirements related to the payment card process environment used for the City. The payment card environment includes any City systems and network that transmit, store, or process payment cardholder data.

Administrative Rule

The City shall abide by all aspects of the current PCI-DSS standard, as set forth by the PCI Security Standards Council (www.pcisecuritystandards.org). PCI-DSS include a variety of general and overarching information security standards that are addressed in other sections of the BTS Administrative Rules; however additional PCI-DSS specific standards are necessary in order for the City to achieve and maintain compliance with PCI-DSS. These standards include but are not limited to:

Encryption of Data

- All payment cardholder data shall be encrypted when transmitted over a public network such as the Internet or the City's internal network. Payment cardholder data is, at a minimum, the sixteen digit primary account number. Cardholder data may also appear in the form of the sixteen digit primary account number plus any of the following: cardholder name, expiration date, or service code.
- Only necessary data and protocols shall be allowed for payment card transactions. All other traffic or protocols are explicitly denied in the payment card environment.

Encryption Key Management

- Knowledge of encryption keys used in the payment card environment shall be restricted to the fewest number of custodians necessary and be based on business need.
- Encryption key custodians are the only personnel authorized to create, distribute, or maintain payment card environment encryption keys.
- Encryption keys must be changed at least annually. The keys may be changed more regularly as necessary and/or as recommended by the associated application.
- All compromised encryption keys must be replaced immediately.
- All encryption keys must be created with the use of strong passphrases in accordance with BTS Administrative Rule 2.05.
- Encryption keys must be strong keys. Strong keys are that meet the minimum recommended key size of comparable strengths recommendations in National Institute of Standards (NIST) Special Publication 800-57, March, 2007. (http://csrc.nist.gov/publications/).
- Encryption keys must not be stored or distributed in clear text. All keys must be encrypted with a key-encryption key.
- Encryption keys must be maintained under a split knowledge and dual control regime.
- Encryption key custodians must sign a key custodian form that recognizes and accepts all key-custodian responsibilities as listed above.

Authentication

- Shared passwords utilized to access any payment card systems or network are prohibited.

Monitoring

- All transaction and activity logs from relevant systems within the cardholder environment shall be reviewed daily.
- Logs from these systems shall be retained for one year from their creation date.
- Logs include, but are not limited to, user identification, type of event, date and time, success or failure indication, origination of event, identity or system component of affected data, or resources.
- Information Security personnel provide 24 X 7 incident response and monitoring coverage for any evidence of unauthorized activity. This coverage shall be manifested in the form of always available communications tools, such as email alerts, that provide readily available information on the status of secure transmission, storage, or processing of payment card data.

Physical Access

- Obsolete paper copies of payment cardholder data must be cross-cut, shredded, incinerated, or pulped once they are no longer needed.
- Physical storage of paper copies of payment cardholder data must be done in a secure environment which includes locked containers.
- End-of-life electronic media used to store payment cardholder data must be purged, degaussed or otherwise destroyed so that cardholder data cannot be reconstructed.
- No payment cardholder data shall be transmitted via end-user messaging technologies including, but not limited, to email and/or instant messaging.
- Storage of all payment card data will be kept only to complete the payment transaction and will not be stored longer than business needs require. At no time after card authorization, under any circumstance, will the City store any information from the card magnetic track, to include Card Validation Value/ Card Validation Code (CVV)/(CVC), CVV2/CVC2, and Personal Identification Number (PIN) block data.
- Account Numbers will be masked when displayed. At any time, the first six and last four digits will be the maximum number of digits to be displayed.
- All media with cardholder data will be audited on a quarterly basis to ensure that stored classified data does not exceed business retention requirements and the retention schedule is adhered to.

System Development Life Cycle

- Software patches to payment card software must be properly tested before being deployed into production.
- Test/development environments must be separate from the production environment, with access controls in place to enforce such separation.
- Test/development personnel must employ separation of duties from production environment personnel.
- Production data (such as active primary account numbers) are not to be used for testing and development, or are sanitized before use.
- Test cardholder data and accounts must be removed before a production system becomes active.
- Custom application accounts, usernames and/or passwords must be removed before a payment card system is placed into production.
- Custom software code for payment card processing must be reviewed prior to release to production in order to identify any potential coding vulnerabilities.
- Software code reviews must be conducted by an individual other than the code author.
- Development of all web applications should be based on secure coding guidelines such as the Open Web Application Security Project Guidelines (OWASP) and PCI-DSS Requirement 6.5.

General Payment Card Security

- The City shall conduct an annual risk assessment of its payment card environment. Involved parties shall be the Data Custodian, and the Information Security Office.
- The Information Security Office shall conduct an annual review of its security policy as it relates to the payment card environment and update the policy whenever changes in the cardholder environment or PCI rules necessitate a change.
- Only devices authorized by the Information Security Office shall connect to any payment card systems.
- All modems must automatically disconnect after 15 minutes of inactivity
- No cardholder data may be stored or copied onto any personal computers or other media not used as part of a centralized backup data solution.
- All payment card systems and/or devices that transmit, store, or process cardholder data must be properly labeled with the current owner, contact information, and purpose of the system or device.
- A current list of all systems or devices that transmit, store, or process cardholder data shall be maintained by the Data Custodian and Information Security Office.

The physical locations for all payment card systems or devices shall be reviewed and approved by the Information Security Office.

- Vulnerability scanning will be conducted on a regular basis for PCI scope devices including but not limited to desktops, servers and network devices. Any PCI scope devices that are discovered to have vulnerabilities shall be remediated according the schedule enumerated in the BTS IT 17.03 Patch Management Standards.

HISTORY

Adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD May 5, 2009.
Revised rule adopted by Chief Administrative Officer of Office of Management and Finance and filed for inclusion in PPD April 17, 2012.
Revised rule adopted by Chief Technology Officer November 15, 2013.