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) for permission to process electronic payments using various payment cards.

This administrative rule outlines specific PCI DSS requirements related to the payment card process environment used by the City. The payment card environment includes any City systems and networks 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. 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 passwords in accordance with BTS Administrative Rule 2.05.
- Encryption keys must be strong keys. Strong keys are keys that meet the minimum recommended key size of comparable strengths recommendations in National Institute of Standards (NIST) Special Publication 800-57 Part 3, March, 2007; Revision 1 January,2015. (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.
- Store cryptographic keys in the fewest possible locations.

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.
- Where a system allows, audit trails shall be implemented and kept to link all access to system components to individual users.
- 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 or text 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 electronic and physical media containing 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.
- 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.
- Physical access to equipment processing cardholder data must be restricted. Access must be authorized and based on individual job function, and be revoked immediately upon termination, including but not limited to the recovery or disabling of all keys, access cards, etc.

Stored Cardholder Data

- Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data irretrievable upon completion of the authorization process.
- Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
- Do not store the personal identification number (PIN) or the encrypted PIN block.
- Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following:

    - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
    - Processes for secure deletion of data when no longer needed
    - Specific retention requirements for cardholder data
    - A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention

- Payment Account Numbers shall be masked when displayed. At any time, the first six and last four digits shall be the maximum number of digits displayed.
- Render Payment Account Numbers unreadable where stored (including on portable digital media, backup media, and in logs) through one-way hashing, tokenization or encryption.
- If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

System Development Life Cycle

- Software patches to payment card software must be properly tested before being deployed into a production environment.
- Test/development environments must be separate from the production environment, with access controls in place to enforce separation.
- Test/development personnel must employ separation of duties from production environment personnel.
- Production data (such as active primary account numbers) shall not to be used for testing and development. Production data must be sanitized before test or development 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.
- Custom software code reviews must be conducted by an individual other than the code author.
- Development of all web applications must be based on secure coding guidelines such as the Open Web Application Security Project Guidelines (OWASP) and PCI DSS Requirement 6.5.
- Software applications (including web-based administrative access to applications) must be developed securely in accordance with PCI DSS, based on industry standards and/or industry best security practices, and incorporate information security throughout the software development life cycle.

General Payment Card Security

- The City shall conduct an annual risk assessment of its payment card environment. Involved parties shall be the Data Custodian, BTS infrastructure service and systems teams, 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 at least annually and approved by the Information Security Office.
- Time synchronization technology shall be used to maintain a correct and consistent time within critical systems. Changes to time configuration must be protected and initiate an alert.
- Vulnerability scanning will be conducted on a regular basis regularly and after any significant change 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.

- Public-facing web applications must be assessed and protected against new threats through vulnerability security assessments at least annually, or an automated technical solution that detects and prevents web-based attacks.

Maintaining Service Providers

- Business owners shall maintain a list of service providers involved with PCI systems.
- Business owners shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the City's cardholder data environment.
- Business owners must establish a program to monitor service providers' PCI DSS compliance status at least annually.
- Business owners must maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the City of Portland.

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 the Chief Administrative Officer of the Office of Management and Finance and filed for inclusion in PPD October 29, 2015.
This rule was reviewed as part of a periodic review and remains unchanged. July 13, 2017.
This rule was reviewed as part of a periodic review and remains unchanged. August 20, 2018.