BTS-2.17 - Payment Card Security Standards

Administrative Rules Adopted by Bureaus Pursuant to Rule Making Authority (ARB)

Policy category: Information Security

Policy number: BTS-2.17

PAYMENT CARD SECURITY STANDARDS

Administrative Rule Adopted by Office of Management and Finance Pursuant to Rule-Making Authority

ARB-BTS-2.17

Search Code, Charter, Policy

Keywords

Search

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. 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.

Revised by Chief Technology Officer October 10, 2018.

This rule was reviewed as part of a periodic review. September 1, 2021.

Related documents

BTS-2.17 Payment Card Security Standards 128.55 KB

BTS-2.17 - Payment Card Industry Data 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 payment card process environments managed and secured by the City and Authorized Third-Party PCI Payment Processors City payment card environments include any City systems, networks, applications and services that transmit, store, or process City payment cardholder data.

Administrative Rule
The City and its PCI Payment Processors must meet all applicable requirements of the current PCI DSS standard, as set forth by the PCI Security Standards Council (www.pcisecuritystandards.org)The 'in-scope' requirements are determined by one or more Self-Assessment Questionnaire (SAQ) types depending on the modes and means of services within each payment card environment.
https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf

Bureaus that use City-approved PCI Payment Processors for electronic payment processing services must use only services and software that are Payment Application Data Security Standard (PA DSS) compliant.

PCI DSS includes a broad expanse of general and overarching information security standards, technology controls, and behavioral expectations that are addressed in other City Administrative Rules of Bureau of Human Resources, Office of Management and Finance, and additional Administrative Rules.

Citywide Technology Standards for PCI DSS Compliance
The following PCI DSS Citywide technology and process standards are required for the City to achieve and maintain compliance with PCI DSS. These standards include but are not limited to:

Payment Card Services Roles and Responsibilities

1. The City is required by the PCI Council to contract with an external PCI-certified auditor to conduct annual risk and compliance assessments of the City's payment card environments.
2. The City is also required contracts for an annual independent PCI DSS compliance audit and quarterly network scans of all bureaus, technologies, and platforms that process electronic payments.
3. The City is also required to annually confirm and collect Attestations of Compliance (AOCs) from all City Authorized Third-Party PCI Payment Processors.
4. Active City participants in PCI risk assessments include each PCI service Business System—or service—Owner (Bureau or Office), Data Custodian (Merchant ID Manager (MID Manager), OMF Treasury Division, BTS Support Professionals - BTS Support Staff, and the Information Security Office.
5. The City Treasury Division is the PCI program service owner and the Information Security Office is the technical controls compliance process owner.
6. Each bureau that provides payment card services or supports a payment card environment must develop and maintain service-specific policies, processes, procedures, training, and security controls to maintain PCI compliance for services within their scope of responsibilities.
7. The Information Security Office must conduct an annual review of its security policy as it relates to City payment card environments and update the policy whenever changes in the cardholder environments or PCI rules necessitate a change.

Authorized Third-Party PCI Payment Processors

1. Business Systems Owners and the OMF Treasury Division must maintain a current list of Authorized Third-Party PCI Payment Processors.
2. Business Systems Owners and the OMF Treasury Division must maintain a written agreement that includes an acknowledgement that Authorized Third-Party PCI Payment Processors are responsible for the security of cardholder data they possess or otherwise store, process or transmit on behalf of the City.
3. Business System Owners and the OMF Treasury Division must establish a program to annually confirm Authorized Third-Party PCI Payment Processors' PCI DSS compliance status.
4. Business System Owners and the OMF Treasury Division must maintain information about which PCI DSS requirements are managed by each Authorized Third-Party PCI Payment Processors, and which are managed by the City of Portland.

Authentication

1. Shared passwords are prohibited to access any payment card environment, system, application, service or Trusted Networks.

Activity and Log Monitoring and Incident Response

1. All Authorized Users must report Information Security Incidents immediately to the BTS Helpdesk. BTS support staff will help you assess the problem and determine how to proceed. See: BTS-2.08 Incident Reporting & Response:

https://www.portlandoregon.gov/citycode/article/699939

2. Information Security personnel and BTS Support Professionals - BTS Support Staff provide 24 X 7 Incident Response and monitoring coverage for any evidence of unauthorized activity or Information Security Incidents. This monitoring coverage includes resilient communications tools, such as email or text alerts, that provide timely information on the status of secure transmission, storage, or processing of payment card data.
3. All transaction and activity logs from relevant systems within the City payment card environments must be reviewed daily.
4. Logs from payment card environments systems must be retained for one year from their creation date.
5. Logs include, but are not limited to, user identification, type of event, date and time, access success or failure indication, origination of an event, identity or system component of affected data, or resources.
6. Payment card environment systems or services that support event correlation must maintain audit trails to associate all access to system components or services with Authorized User accounts.

Physical Access

1. 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.
2. Storage of all payment card data in electronic systems or physical media 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, the Card Validation Value/ Card Validation Code CVV/CVC, CVV2/CVC2, or the Personal Identification Number (PIN) block data.
3. Paper copies of payment cardholder data must be cross-cut, shredded, incinerated, or pulped once they are no longer needed.
4. Physical storage of electronic and physical media containing payment cardholder data must be secured in locked containers within physically secured, non-public-access, workspaces.
5. End-of-life electronic media used to store payment cardholder data must be purged, degaussed or destroyed so that cardholder data cannot be reconstructed.
6. All electronic systems and physical media with cardholder data will be audited on a quarterly basis to ensure that stored classified data does not exceed business retention requirements and that the retention schedule is adhered to.

Payment Card Services Device Management

1. Only devices authorized by the Information Security Office must connect to City managed payment card systems, applications, services or environments.
2. Bureaus that use payment card devices to process payment card transactions must use only devices that meet PCI PIN Transaction Security (PTS) validation and utilize point-to-point encryption technology.

3. All payment card environment modems must automatically disconnect after 15 minutes of inactivity.
4. All payment card systems, devices, applications or services that transmit, store, or process cardholder data must be properly inventoried, secured, and where appropriate, labeled.
5. The OMF Treasury Division maintains the Citywide database of authorized payment card processing environments, devices, current Business System or Service Owner, MID Managers, Merchant IDs, and Authorized Third-Party PCI Payment Processors
6. MID Managers are responsible to provide the OMF Treasury Division with all payment card services information and all changes within their payment card environment, including, but not limited to: contact information, and purpose of the system or device.
7. Payment cardholder data is prohibited from transmission via end-user messaging technologies including, but not limited to, email or text messaging.
8. A current list of all systems or devices that transmit, store, or process cardholder data must be maintained by each Bureau, Office or MID Manager and the OMF Treasury Division.
9. The physical locations for all payment card systems or devices must be reviewed at least annually and approved by the Information Security Office.
10. Time synchronization technology must be used to maintain a correct and consistent time within critical systems. Changes to time configuration must be protected and initiate an alert.
11. 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 must be remediated according the schedule enumerated in the BTS Patch Management Standards. See: City of Portland Information Security Standards
12. 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.

Stored Cardholder Data

1. Retention or storage of authentication data after authorization--even if encrypted—is prohibited. When authentication data is received, render all data irretrievable upon completion of the authorization process.
2. Retention or storage of any cardholder data from a chip or magnetic track-- the magnetic stripe located on the back of a card–is prohibited.
3. Retention or storage of the personal identification number (PIN) or the encrypted PIN block is prohibited.
4. Retention of any permitted cardholder data must be securely stored by implementing data retention and disposal policies, procedures and processes that include at least the following:
    a. Limiting data storage content and retention time to that which is required for legal, regulatory, and business requirements

b. Establishing and maintaining processes for secure deletion of data when no longer needed
c. No permitted cardholder data may be stored or copied onto personal computers or any other media not used as part of a centralized and BTS-approved backup data solution
d. Defining and auditing compliance with specific retention requirements for permitted storage of cardholder data
e. Quarterly automatic or manual processes for identifying and securely deleting stored cardholder data that exceeds defined retention periods

5. Payment Account Numbers must be masked when displayed. At all times, the first six and last four digits must be the maximum number of digits displayed.
6. Render Payment Account Numbers unreadable where stored (including on Removable Media, backup systems, and in logs) through one-way hashing, tokenization or encryption.
7. If disk-level 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 Authorized User account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Encryption of Data

1. All City Merchant ID (MID) payment cardholder data must be encrypted when transmitted over a public network such as the Internet, and within the City's Trusted Networks. 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.
2. Only necessary data and secure protocols are permitted for City payment card transactions. All other traffic or protocols are explicitly denied in City payment card environments.

Encryption Key Management

1. City Authorized Users are prohibited from knowing or having access to the encryption keys used by the City's PCI Payment Processors or the manufactures of point-of-sale payment devices.
2. Only authorized encryption key custodians are authorized to create, distribute, or maintain City payment card environment encryption keys.
3. All City managed encryption keys must only be created by authorized encryption key custodians using Administrative Accounts and the use of strong passwords in accordance with BTS Administrative Rule 2.05 Authorized User & Administrative Passwords.
4. Knowledge of City managed encryption keys used in payment card environments must be restricted to the fewest number of custodians necessary and be based on business need.
5. Cryptographic keys must be stored in the fewest possible locations.
6. Encryption keys must not be stored or distributed in clear text.
7. All encryption keys must be encrypted with a key-encryption key.

8. Encryption keys must be maintained under a Split Knowledge and Dual Control Regime.
9. City managed encryption keys must be changed at least annually. The keys may be changed more regularly as necessary or as recommended by the associated application or business use care.
10. All compromised encryption keys must be replaced immediately.
11. City managed encryption keys must use BTS and PCI DSS approved algorithms.
12. Encryption key custodians must sign a key custodian form that acknowledges and accepts all encryption key management responsibilities as listed above.

System Development Life Cycle

Payment Card Services System, Application and Service Development

1. Payment processing systems, services and application development must be developed securely in accordance with PCI DSS, based on industry standards and/or industry best security practices for secure coding, and incorporate information security throughout the software development life cycle.
2. Software patches to payment card systems, services and applications must be properly tested before being deployed into a production environment.
3. Test and development environments must be separate from the production environment, with access controls in place to enforce separation.
4, Custom and default application accounts, usernames and passwords must be removed before a payment card system is placed into production.
5. Test and development Authorized Users must employ separation of duties from production environment Authorized Users.
6. Test cardholder data and accounts must be removed before a production system becomes active.
7. Custom software code for payment card processing must be reviewed prior to release to production to identify any potential coding vulnerabilities.
8. Custom software code reviews must be conducted by an individual other than the code author.
9. Production data, such as active primary account numbers, must not to be used for testing and development. Production data must be sanitized before test or development use.

References

Please refer to the following BTS resources for term definitions, acronyms, and BTS standards used within BTS Admin Rules:

1) BTS Technology Definitions – https://www.portlandoregon.gov/citycode/article/114449
2) (BTS) Technology Standards Directory (and Acronyms) -- https://www.portlandoregon.gov/bts/article/44978
3) City of Portland Information Security Standards

Several OMF Bureau of Revenue and Financial Services' Administrative Rules apply to PCI and payment card process environments:

1) FIN-2.10 - Electronic Payment Processing Services
https://www.portlandoregon.gov/citycode/article/200854

2) FIN 2.10.01 Guidelines for Electronic Payment Processing Services
https://www.portlandoregon.gov/brfs/article/531056

3) FIN 2.10.02 Technical Requirements for Electronic Payment Processing Services
https://www.portlandoregon.gov/brfs/article/531062

4) FIN 2.10.03 Best practices for Processing Payment Card Transactions
https://www.portlandoregon.gov/brfs/article/531069

5) FIN 2.10.04 Security of Payment Device Hardware
https://www.portlandoregon.gov/brfs/article/563271

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.
This rule was reviewed and revised as part of a periodic review. September 2, 2019.
This rule was reviewed and revised as part of a periodic review. June 30, 2020.
This rule was reviewed as part of a periodic review. September 1, 2021.