Document Code No.: FIN-8-10-EP
Title: Payment Card Processing and Data Security Standard Compliance Policy
Affected Agencies: Any Offices and Departments that use and process payment card information
Authorities: RCW 19.255.020, RCW 36.29.190, King County Code Title 2A.380, FIN-8-5-2-EP, ITG-P-21-04, ITG-P-21-01, ITG-P-21-06, ITG-P-21-10, Ordinance 20012
Keywords: PCI DSS Compliance, Cardholder Data Protection, Payment Card
Sponsoring Agency: King County FBOD

King County

Executive signature: Signed by: Girmay Zahilay B7B9CFF6992F49A...
Date signed and effective: 5/6/2026

I. Purpose

The Payment Card Industry Data Security Standard (PCI DSS) is a mandatory set of requirements developed by the major credit card brands (Visa, MasterCard, Discover, American Express, and JCB). These standards apply to all Merchant Departments that store, process, or transmit cardholder data.

The purpose of this policy is to establish King County's requirements for handling, processing, transmitting, storing, and disposing of cardholder data, and to protect customer cardholder data entrusted to King County. This policy applies Countywide to all Merchant Departments that use, process, or transmit payment card information to ensure compliance with this regulation.

The County will protect customer cardholder data through:

- Ensuring compliance with PCI DSS and other applicable state, federal, and County requirements.
- Defining and executing the governance structure for PCI compliance within King County.
- Clarifying responsibilities of the Finance and Business Operations Division (FBOD), County Merchant Departments, KCIT Security & Privacy, and applicable third parties including payment processing services.
- Reducing risk exposure through consistent controls, monitoring, reporting, and accountability.

II. Applicability and Audience

This policy applies to all King County Merchant Departments, including all workforce members such as employees, contractors, interns, volunteers, and third parties who handle, process, transmit, store, or manage payment card transactions or cardholder data on behalf of King County using the Enterprise Payment Card Service Provider, or approved Third-Party Merchant Service Provider.

All workforce members that process payment card transactions as a Merchant are responsible for ensuring compliance with the latest version of PCI DSS. This policy does not apply to payment cardholders or groups that are not considered Merchants under PCI DSS, such as a P-card holder for the purposes of accounts payable payments.

This policy supplements FIN-8-5-2-EP, and established authorities under FIN-8-5-2-EP or its successor policy remain in full effect, except for roles and responsibilities outlined for PCI Compliance governed by this policy.

III. Definitions

"CHD", or Cardholder Data, includes the Primary Account Number (PAN) plus any of the following: cardholder name, expiration date, service code.

"CDE" is an acronym for Cardholder Data Environment, which is comprised of the system components, people, and processes that store, process, or transmit cardholder data and/or sensitive authentication data, and system components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

"EPCSP" is an acronym for the Enterprise Payment Card Service Provider, FBOD's selected merchant services provider selected to deliver large-scale electronic payment processing solutions to King County.

"Electronic Business Steering Committee" ("EBSC") (or its successor) refers to the committee of county representatives, chaired by the Finance Director, who provide guidance, advice, and oversight of County electronic payment strategy, and assistance to departments as part of the county's Electronic Payments Management Plan.

"FBOD" refers to the Finance and Business Operations Division

"Merchant" For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any PCI SSC Participating Payment Brand as payment for goods and/or services. A merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an Internet Service Provider is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

"Merchant Department", for the purposes of this policy, is a King County department, agency, or program authorized to accept payment cards and assigned a Merchant ID.

"P2PE" is an acronym for Point-to-Point Encryption, a PCI Security Standards Council-validated encryption standard that protects payment card data by encrypting it immediately at the point of entry.

"PCI DSS" is an acronym for the Payment Card Industry Data Security Standard, published by the PCI Security Standards Council.

"PCI SSC" is an acronym for the Payment Card Industry Security Standards Council

"Point of Interaction (POI) Device" is an approved device where cardholder data is captured.

"QSA" is a Qualified Security Assessor, which is a certified professional or company authorized by the PCI SSC to independently assess and validate PCI DSS

compliance.

"Sensitive Authentication Data "(SAD)", refers to security-related information used to authenticate cardholders and/or authorize payment card transactions. This information includes, but is not limited to, card verification codes, full track data (from magnetic stripe or equivalent on a chip), PINs, and PIN blocks.

"SAQ" is a Self-Assessment Questionnaire, which is a merchant tool to self-report compliance with the PCI DSS (Payment Card Industry Data Security Standard).

"Service Provider" is a third party that stores, processes, or transmits cardholder data on behalf of King County.

"Third Party Merchant Service Provider" or "Third Party Service Provider", for the purpose of this policy, is a company that provides payment services to businesses, allowing them to accept and process payments from customers. Merchant Departments at King County are required to use the Enterprise Payment Card Service Provider, which is compliant with PCI and Credit Card Brand Standards. Departments wishing to contract with a Third-Party Merchant Service Provider must obtain an exception to this requirement under FIN-8-5-2-EP, or its successor policy.

See also PCI-DSS Council Standards Glossary
https://www.pcisecuritystandards.org/glossary/

IV. Policy Requirements

A. Authorized payment card acceptance

1. Merchant Departments at King County are required to use the Enterprise Payment Card Service Provider, which is compliant with PCI DSS requirements. Merchant Departments wishing to obtain an exception to this requirement must refer to FIN-8-5-2-EP, or its successor policy.

2. All credit card processing is subject to audit. This includes credit card payments received via web, online, walk-in, phone calls, mail, and off-site events.

B. Prohibition on storing Sensitive Authentication Data (SAD) after authorization

1. Storage of SAD after authorization is prohibited. Immediately after authorization, SAD must be disposed of securely and promptly. Paper records must be physically destroyed such that cardholder data cannot be reconstructed.

2. Collected cardholder data must be restricted only to those workforce members who need the data to perform their jobs. Each Merchant Department

must maintain a current list of employees with access to it and review the list monthly for any necessary updates, among other things.

3. If a Merchant Department has a legitimate business, legal, or regulatory requirement preventing the destruction of SAD after authorization, that Merchant Department must request an exception through the EBSC or its successor. If an exception is approved by the EBSC, the permitted cardholder data (PAN, expiration date and cardholder date) must be stored in a secure, locked location, and retained for no longer than 3 years.

C. Merchant Department verification of vendor/service provider compliance with PCI DSS

1. Merchant Departments permitted under FIN-8-5-2-EP, or its successor policy, to contract with a Third-Party Merchant Service Provider, are responsible for verifying the provider's PCI compliance in accordance with this policy. As part of these obligations, Merchant Departments must:

a. Verify a Service Provider's PCI compliance status on an annual basis.

b. Retain Attestations of Compliance ("AOC") and compliance evidence for 6 years and evidence must be available upon request to FBOD, KCIT or auditors.

c. Maintain a written agreement that requires the Third-Party Service Provider to be responsible for the security of any cardholder data possessed, stored, processed or transmitted on behalf of the cardholder customer.

D. Administrative Controls implemented by Merchant Departments

1. POI inventories and tamper inspections are to be performed at least annually, to the requirements specified in the PCI Compliance Policy and Operations Manual, once available.

2. Any unauthorized devices should be identified by comparing serial numbers with those of deployed devices. If a variance is discovered when performing the annual POI device inventory, including missing or substituted POI devices, contact the EPCSP immediately.

3. When not in use, devices should be stored securely. Merchant Departments should periodically check for signs of tampering, such as protruding wires, foreign objects in the card slots, missing or altered seals, or additional overlays covering the device or card slots. Additionally, Merchant Departments

should monitor devices for consistently unusual behavior (such as a high volume of read failures) and restrict physical access to devices by third-party technicians.

E. Cardholder Data Technical Protections

It is a requirement that all Merchant Departments ensure technical protection of its cardholder data, through the following technical safeguards:

1. Cardholder data must be protected using strong cryptographic controls when stored, processed, or transmitted over open or public networks. Approved methods for rendering cardholder data unreadable include industry-accepted encryption, truncation, or tokenization, in accordance with PCI DSS requirements.

2. Encryption keys must be protected against disclosure and misuse, with access restricted to only those workforce members or systems with a legitimate business need. Keys must be stored securely, managed in accordance with established County security standards, and rotated or replaced as required.

3. Transmission of cardholder data must use secure communication protocols that meet or exceed PCI DSS encryption standards. Cardholder data may not be transmitted via unencrypted email, messaging platforms, file sharing services, or other unsecured communication channels.

4. Systems that store, process, or transmit cardholder data must implement appropriate technical safeguards to protect against unauthorized access, including network segmentation or isolation, secure configuration standards, and access controls based on least privilege.

5. Strong authentication mechanisms must be used to access payment systems and cardholder data environments, in alignment with County security standards, and may include multi-factor authentication where required or appropriate.

6. Cardholder data environments must be protected through vulnerability management and system security practices, including timely patching, malware protection where applicable, and logging sufficient to support audit, monitoring, and incident response requirements.

7. Changes to payment system configurations, integrations, or software must follow established change management processes, and technical controls must be maintained to prevent unauthorized transmission or disclosure of cardholder data outside approved payment workflows.

F. Responsibilities

1. Finance & Business Operations Division (FBOD)
   a. Own and maintain this Countywide Payment Card Compliance Policy.
   b. Approve and administer Enterprise Payment Card Service Provider Merchant IDs and accounts.
   c. Manage contracts with Enterprise Payment Card Service Provider.
   d. Participate in the annual Countywide PCI DSS compliance reporting and SAQ submissions, as led by KCIT Security & Privacy.

2. KCIT Security & Privacy
   a. Provide PCI DSS consultation, guidance, and technical expertise to Merchant Departments and FBOD.
   b. Lead and maintain risk assessment for primary PCI DSS requirements, including penetration testing, network security controls and configurations, daily log monitoring, authentication/access control, and a vulnerability management program, as needed.
   c. Provide training and awareness materials related to data security, including PCI Compliance.
   d. Lead incident response activities when cardholder data breaches occur, in coordination with FBOD and affected Merchant Departments.
   e. Procure, administer, and maintain contract with a QSA contractor.
   f. Responsible for leading and ensuring the QSA risk assessment and SAQ submissions are completed annually.
   g. Advise and support Merchant Departments implementation of PCI compliant solution architecture for all payment channels.
   h. Maintain documentation and data flow diagrams of Card Holder Data Environments produced by agencies.

3. Departments, Agencies, and Programs (Merchant Departments)
   a. Maintain operational PCI DSS compliance for their payment environments.
   b. Designate a Merchant Department Primary Contact (MDPC) and backup.
   c. Coordinate with KCIT and the contracted QSA to complete and submit annual PCI DSS SAQ and evidence of compliance.
   d. Independently lead corrective measures to resolve gaps, risks and findings identified by the QSA contractor during the annual assessment process
   e. Collaborate with KCIT to produce or update documentation and data flow diagrams of Card Holder Data Environments.
   f. Maintain current POI device inventories and tamper inspection logs.
   g. Ensure applicable staff complete annual PCI DSS training and written policy acknowledgment.
   h. Reconcile merchant and settlement accounts per FBOD requirements.
   i. If approved to enter a contract with a Third-Party Merchant Service Provider, Merchant Departments must ensure PCI Compliance requirements are met in accordance with this policy.

4. Workforce Members

a. Complete PCI DSS training and a policy acknowledgement upon hire and annually thereafter.
b. Use only technologies approved by KCIT for payment card acceptance.
c. Immediately report any suspected or confirmed cardholder data breach.
d. Participate in audits and incident investigations as requested.

5. Enterprise Payment Card Service Provider and Approved Third-Party Merchant Service Providers
   a. Maintain annual PCI DSS compliance and provide Attestation of Compliance (AOC) to Merchant Departments.
   b. Include PCI DSS compliance clauses in contracts.
   c. Support King County in audits and incident investigations as required.

6. Electronic Business Steering Committee
   a. Provide leadership guidance and monitoring for PCI compliance across their Merchant Departments.
   b. Review requests for exceptions to this policy, as recommended by the Finance and Business Operations Division and the Chief Information Security Officer.

G. Implementation Plan

1. This policy becomes effective for Merchant Departments on the date that it is signed by the Executive. As the business owner for electronic payments, the Finance and Business Operations Division is responsible for implementation of this policy in collaboration with KCIT and Merchant Departments.

2. Merchant Department Directors, or their designees, are responsible for communicating this policy and PCI Compliance Policy Operations Manual to the management structure within their respective agencies and other appropriate parties.

3. Merchant Departments and Division Directors are required to develop and implement supplemental policies and procedures to ensure PCI/DSS compliance, as needed to ensure compliance.

H. Maintenance

1. This policy will be maintained and reviewed annually by FBOD, or its successor agency, and updated as needed to reflect PCI DSS changes or King County requirements.

2. This policy will automatically expire five (5) years after its effective date. A new, revised, or renewed policy will be initiated by the Finance and Business Operations Division, or its successor agency prior to the expiration date.

I. Exceptions

1. Any request for exception must be submitted in writing to FBOD. Exceptions are reviewed on a case-by-case basis at the EBSC and require written approval by the Finance and Business Operations Division and the Chief Information Security Officer, in collaboration with the Department Director, or their successor agencies or delegates. Written exceptions are valid for one year and must be reviewed annually at the EBSC.

V. Consequences for Noncompliance

1. King County has a fiduciary and legal responsibility to protect cardholder data when processing payment card transactions. Non-compliance with PCI DSS may result in financial penalties, reputational damage, suspension or revocation of merchant accounts, and/or loss of the ability to process payment cards.

2. Non-compliance with this policy may result in:
   a. Loss of payment card processing privileges for the department or agency.
   b. Financial penalties and reimbursement of fines imposed on King County.
   c. Disciplinary actions for employees, up to and including termination.
   d. Contract termination for third-party vendors and service providers.

Appendices:

A. PCI DSS v4.0 (PCI Security Standards Council)
   1. https://www.pcisecuritystandards.org/standards/pci-dss/
   2. https://www.pcisecuritystandards.org/glossary/
B. King County Information Security Policy
C. King County Incident Response Plan
D. Grant Street Group-King County Listed P2PE Merchant Responsibilities
E. PCI Compliance Policy Operations and Procedure Manual
F. Contracting with Vendors to Accept or Process Payments, WA State Auditor, 5/2025
   1. https://sao.wa.gov/sites/default/files/2023-05/contracting-with-third-party-vendors-payment-processing.pdf