| **Procedure**<br>Credit Card Processing Vendor Evaluation, Contracting, and Management | **Effective Date:**<br>January 1, 2020<br>**Adoption/Revision Date**<br>January 1, 2020 |
|---|---|

References: Credit Card Payments; Vendor Remote Access Request Form

Procedure Custodian: Information Security Advisory Committee (ISAC)

Purpose: To provide procedures for the evaluation, contracting and on-going management of vendors that provide credit card processing services and devices to Jefferson County. These procedures are important to protect the integrity and protection of credit card information provided by the public to pay for Jefferson County services and to provide for compliance with requirements (PCI-DSS) of the credit card industry.

A. Definitions

1. Authorized Employees, Volunteers, or Contractors: County elected or appointed officials, employees, including Information Technology staff responsible for county networks and systems, volunteers or contractors that handle or process CCD or work in the CDE for a county Department/Division or Elected or Appointed Office and have undergone a thorough background check.

2. Cardholder Data Environment (CDE): The Cardholder Data Environment consists of the networks, web sites, devices, processes, and individuals who directly interact with Credit Card Data or with consumers submitting Credit Card Data for processing.

3. Credit Card Data (CCD): Full magnetic stripe data from the credit card or the Primary Account Number (PAN), plus any of the following: cardholder name, expiration date, or security code

4. Merchant Account: A relationship set up between the county and a credit card processing vendor in order for the county to accept credit card transactions. The vendor provides a Merchant ID number to tie payments to the Treasurer's general ledger account to distribute funds appropriately to the Department/Division or Elected/Appointed Office for which the account was established.

5. Payment Card Industry Data Security Standard (PCI DSS): A proprietary information security standard for organizations that handle branded credit cards from the major card companies including Visa, Master Card, American Express, Discover and JCB (Card Brands). The standard was created to increase controls around cardholder data and to reduce credit card fraud via exposure of that data.

6. Primary Account Number (PAN): The credit card number (credit or debit) that identifies the issuer and the specific cardholder account. Also called the Account Number.

7. Security Code: A 3 or 4-digit code found on the back or front of the credit card. Also known as the CVV, CID, CAV2, CVC2, or CVV2 code.

8. Self-Assessment Questionnaire: The PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool used by merchants to demonstrate compliance with PCI DSS.

9. Vendor Management Employees: County employees who participate in the evaluation, contracting and ongoing vendor management processes involving service providers for the processing of credit card payments, provision of credit card devices or other related services.

B. Applicability

1. Departments/Divisions that report to the Board of County Commissioners, Elected Officials Offices and, Appointed Officials Offices.

2. This procedure is in addition to the Purchasing Policy and Procedures.

C. Compliance with Industry Standards

1. The Finance Director will approve the selection of one or a small number of credit card processing vendors with the goal of reducing administrative and technical overhead expenses for vendor management and complying with industry requirements while addressing the business needs of the county.

2. Vendor Evaluation

   a. The Safety and Compliance and Business Innovation and Technology (BIT) Divisions will evaluate:
      (1) On-line processing capabilities and security
      (2) Design of websites linking to a vendor's on-line services
      (3) Selection of card swipe devices
      (4) Any use of card swipe devices with mobile devices (e.g., smartphones and tablet)
      (5) Connections of credit card devices to Jefferson County wired and wireless networks
      (6) Business requirements for handling credit card information

   b. The following special evaluation criteria will be considered:
      (1) Does the vendor utilize criminal background checks for all positions that create software or in any way handle or have access to credit card information? The vendor should be asked to provide a summary description of their internal controls environment.
      (2) Examination of a summary description of the vendor's internal controls environment.
      (3) If the vendor utilizes sub-contractors or third party service providers, what controls do they utilize to ensure their compliance with PCI DSS?
      (4) Has the vendor failed to meet PCI DSS compliance criteria within the past 5 years?
      (5) Has the vendor had any credit card breaches (lost data) within the past 5 years?
      (6) What is the vendor's current status as a Payment Card Industry approved company/provider?
      (7) What capabilities does the vendor have to provide disaster recovery/business

continuity for the services?

3. The amount of diligence performed in vendor selection will increase with the amount of risk associated with the outsourced solution. When justified by the vendor risk assessment, the Finance Division, with support from Safety and Compliance and BIT, will critically examine the vendor's internal control environment to ensure acceptable levels of risk can be maintained during service delivery. Some relevant aspects of a vendor's internal control environment should include:

    a. Organizational security policies and procedures

    b. Information security architecture documents

    c. Employee background, credentials, certifications, and education

    d. Risk assessment documentation

    e. SAS-70 Type I or II audit documents

D. Vendor Contracting

1. Contracts must include the following:

    a. Acknowledgement of the vendor's possession of cardholder data. The vendor shall acknowledge that such data can only be used for assisting the Card Brands or banks in completing a transaction, supporting a loyalty program, providing fraud control services, or for uses specifically required by law.

    b. Confirmation that all third-party vendors and vendors' licensors or any third party companies used by the vendor involved in credit card transactions meet all PCI DSS standards; acknowledge their responsibility for safeguarding the cardholder data they possess, store, process or transmit; and provide to the County proof of compliance by providing an Attestation of Compliance.

    c. If processing or storing credit card data on behalf of the county, vendors must protect cardholder data as specified by the most current version of PCI DSS, and submit proof of PCI DSS compliance status prior to contract approval and at least annually (e.g., QSA report).

    d. Requirement to report any known or suspected compromise/loss of CCD to the county within no more than 10 business days after the compromise/loss is detected.

    e. Permission to audits by Card Brands in the event of a CCD compromise.

    f. Agreement to continued security of CCD during and after contract terminations. Contracts shall require return or secure destruction of all county CCD in accordance with the vendor's information classification and handling policies provided those policies are acceptable to the County.

g. Provision of appropriate business continuity capabilities such that the services provided by the vendor will be available in the event of a major disruption or failure of their primary facilities.

h. Definition of Service Level Agreements for both normal and contingency operations.

2. Cyber Security Insurance

   a. The vendor shall maintain, at its own expense, insurance ("Insurance") to cover itself for claims, losses, liabilities, judgments, settlements, lawsuits, regulatory actions, and other costs or damages arising out of its performance under the contract with the county, including any negligent or otherwise wrongful acts or omissions by the vendor or any employee or agent thereof. This includes, but is not limited to, any breach of the PCI DSS.

   b. The policy or policies comprising said Insurance shall together provide limits of liability of at least $2 million in the aggregate.

   c. Upon the county's request, the vendor or the vendor's agent shall provide the county with a copy of all certificates or verifications of insurance evidencing the existence of Insurance coverage required hereunder.

   d. The vendor shall require the carriers for such Insurance to provide, and the vendor shall provide the county notice of not less than thirty (30) days prior written notice of any material change in: (1) the Insurance policy of the vendor and (2) the status of said Insurance policy, including but not limited to cancellation, non-renewal or extension with regard to any insurer participating on the Insurance, regardless of the reason thereof.

3. Vendor Local and Remote Access to the county CDE

   In the case a vendor requires local or remote access to troubleshoot, access, or support a service or device in the county-owned CDE, the vendor must:

   a. Submit the "Vendor Request for Remote/Local Access to Jefferson County Cardholder Data Environment" included in this procedure. The request shall provide the individual names of those individuals requiring access; no shared accounts will be allowed.

   b. Agree that accounts are temporarily enabled for only the time of use and disabled all other times.

   c. Access systems and networks only on a "need-to-know" basis with access limited to only that needed to perform their job function (Principle of least Privilege).

   d. Require its employees to sign an agreement protecting the confidentiality of county information.

   e. BIT must approve any remote access to the county CDE.

(i) Remote access technologies used by vendors includes, but is not limited to TeamViewer, VNC, Remote Desktop, and GoToMyPC.

(ii) Immediately notify Safety and Compliance and BIT if vendors or outside parties require remote access, or if you notice that vendors or outside parties are remotely accessing your workstations or devices that handle credit card information.

(iii) BIT will provide two-factor authentication for the vendor's remote access during the interval when access is required.

f. Acknowledge that:

(i) BIT will monitor the vendor's remote and local access to county-owned systems, hardware, software and data.

(ii) All vendor access (remote and local) to the CDE will be manually observed by an Authorized Employee, Volunteer or Contractor or recorded via software.

(iii) The county will terminate all access to facilities, services, systems and data immediately upon termination of the service contract/agreement. Upon termination of a Credit Card Processing vendor's services, the vendor will return all security artifacts and CCD to the Finance Division. This may include data and documents.

E. On-Going Vendor Management

1. The Finance Division will maintain a Credit Card Processing Vendor Management Program by performing a thorough and diligent selection of available vendors and perform ongoing monitoring of vendor performance against business and contractual requirements.

2. The Finance Division shall maintain an up-to-date list of all currently approved service providers, the services/devices provided, and the Merchant IDs assigned by the respective Departments/Divisions or Elected/Appointed Offices. It is the responsibility of the Finance Division, with assistance from BIT, to periodically review the financial condition, stability, system security, recovery plans/testing, security assessment tests, internal control practices, and PCI DSS compliance of all credit card processing vendors and service providers in use by the county.

2. It is the responsibility of Finance Division to maintain a copy of each vendor's most recent compliance documents (i.e., AOC or QSA reports).
3. It is the responsibility of the Safety and Compliance Division to verify the vendor's compliance documents align with contractual requirements.

4. The Finance Division shall maintain current evidence of PCI DSS compliance for any Third Party Services/Companies used by each Credit Card Processing service providers with whom CCD is shared as per the PCI DSS.

5. The Finance Division will ensure that all PCI DSS documentation is maintained in hard copy form in a separate binder for each Credit Card Processing service provider and kept in a secured county office. Electronic copies of all PCI DSS documents are retained permanently.

6. The Finance Division will provide immediate notification for BIT to terminate all access to facilities, data, systems, and applications immediately upon termination of a vendor's service agreement/contract in accordance with the county's access control procedures, standards, and/or other documents.

7. SAQs will be completed by Safety and Compliance. No other Division/Department or Elected/Appointed Office is authorized to submit a SAQ to a credit card processing vendor or industry association on behalf of the County. Safety and Compliance will establish a procedure for the annual collection and submittal of information to comply with industry requirements.