Procedure Credit Card Handling and Security for Departments/Divisions and Elected/Appointed Offices	**Effective Date** January 1, 2020 **Adoption/Revision Date** January 1, 2020

References: Credit Card Payments Policy

Procedure Custodian: Information Security Advisory Committee (ISAC)

Purpose: To comply with the Payment Card Industry Data Security Standards (PCI DSS)

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 credit card companies including Visa, Master Card, American Express, Discover and JCB (Card Brands). The standard was created to increase controls around CCD 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. Self-Assessment Questionnaire (SAQ): The PCI DSS Self-Assessment Questionnaire (SAQ) is a validation tool used by merchants to demonstrate compliance with PCI DSS.

8. 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, CVV2 or service code.

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. Authorized Employees, Volunteers, or Contractors

3. Authorized Vendor Management Employees

4. The Safety & Compliance Division shall review and update this Procedure at least annually. Each Authorized Employee, Volunteer or Contractor will be required to confirm that they have read, understand and agree to abide by these procedures and any applicable procedures, standards and/or other documents.

C. Devices and Web Sites

1. Per the Credit Card Payment Policy, Safety & Compliance, BIT and Finance Directors must approve all credit card processing proposals prior to entering into any contract, purchasing services or equipment, adding Merchant Accounts or installing, moving or permanently disconnecting any credit card devices. This shall apply regardless of the transaction method, such as online processing, swipe terminals, desktop/laptop computers or mobile devices and whether wired or wireless.

2. Labels must be affixed to all credit card processing devices (e.g., asset tag or other label to identify Jefferson County) to verify that the device is a legitimate county device.

3. All unnecessary accounts, services, and other functionality must be removed from or disabled on systems and desktop/laptop computers before they are used to process or store CCD.

4. Credit card PANs must not be entered into the web page of a server hosted on Jefferson County networks. PANs should only be entered onto the web page provided by an approved credit card processing vendor.

5. All credit card processing devices must be programmed to print out only the last four or first six characters of a credit card number.

D. Handling and Processing Credit Cards

1. In Person (Standard and mobile terminals)

   a. When possible, do not handle the credit card. Ask the customer to swipe the credit card and to show you the credit card if needed. If handling the credit card is required due to the location of the credit card device or other factors, keep the credit card in view of the customer at all times.

b. If the credit card is not signed, ask the customer for a photo ID.

c. Process the transaction immediately.

d. If the customer needs to give you the credit card to be swiped, do not give the credit card back to the customer until the payment is approved. When possible, avoid the need to handle the credit card.

e. Once the transaction is completed, compare the signature on the receipt to the back of the credit card. If the credit card is not signed, compare the signature against the signature on a photo ID.

f. If the credit card is declined, request another form of payment.

2. Paper Transactions

a. Credit card information shall not be written down at any time, including having credit card information submitted via paper mail. Your management can contact Safety & Compliance, Finance and BIT to consider alternate credit card payment methods such as online or automated voice systems.

b. If credit card devices or systems are not working and preventing credit card information from being directly entered into a credit card terminal or website, it is recommended that the customer be asked to come back when the system is up.

c. If the Department/Division or Elected/Appointed Office's management gives approval to accept and/or store CCD on paper, the business justification and approval must be documented and kept in the Credit Card Standards Manual.

d. If a credit card is declined, call the customer immediately and make a note on the customer's account if services were already rendered.

e. Print receipts for the customer and the county; mail the customer a copy of the receipt and store the county copy in a secured location.

3. Telephone Transactions

a. It is recommended that credit card information not be accepted by telephone. Your management can contact Safety & Compliance, Finance and BIT to consider alternate credit card payment methods such as online or automated voice systems.

b. If credit card information must be accepted over the telephone with the customer, immediately process the credit card information while on the phone by entering it directly into a credit card device. Do not write down or save the CCD in an electronic file on a computer. While on the phone, ask the customer to repeat the credit card number and expiration date back to you; do not repeat the credit card information back to the customer.

c. Ask for a return phone number.

d. Keep the customer on the phone until the transaction has been approved.

e. Print a receipt/invoice for county records and mail a copy to the customer.

f. If you had to write down any CCD, shred the information once the transaction has been completed.

g. Calls involving CCD should not be forwarded to anyone except another Authorized Employee, Volunteer or Contractor in your Department/Division or Elected/Appointed Office.

h. Three-way calling should never be used if the call involves CCD.

4. Fax Transactions

   a. It is strongly recommended that credit card information not be accepted by Fax at any time. Your management can contact Safety & Compliance, Finance and BIT to consider alternate credit card payment methods such as online or automated voice systems.

   b. If the Department/Division or Elected/Appointed Office's management gives approval to accept and/or store CCD on paper, the business justification and approval must be documented and kept in the Credit Card Standards Manual.

   c. If credit card devices or systems are not working preventing credit card information from being directly entered into a credit card device or website, it is recommended that the customer be asked to call back when the devices or system is working.

   d. Ensure the fax machine is located in a secure environment that can only be accessed by Authorized Employees, Volunteers, or Contractors.

   e. If a credit card is declined, call the customer immediately and make a note on the customer's account if services were already rendered.

   f. Print receipts for the customer and the county; mail the customer a copy of the receipt and store the county copy in a secured location.

5. Email Transactions

   a. Never send or ask to receive CCD using unencrypted end-user messaging technologies, such as instant messaging, email, text message, etc.

b. Encrypted email systems may be used to send or receive CCD, but such messages should never be stored on a computer.

c. If a customer sends CCD in this way, immediately enter the CCD in to a credit card device or system, securely delete the message and shred any paper printout of the message. This can be accomplished by first deleting the email and then opening your “Deleted Items” folder and again deleting the email from that folder. Notify the customer of alternate ways of paying by credit card. Never include any CCD in replies to the customer.

6. Internet Transactions
Ensure that any websites that offer credit card payment have been reviewed and approved by Safety & Compliance and BIT.

7. Recurring Payment Transactions

a. Have your management review the contract with the credit card processing vendor. Some vendors, such as Square, prohibit recurring payments.

b. “Tokenization” should be used for processing recurring payments instead of storing credit card information. The “token” can be used to process future payments and does contain confidential CCD. Contact Safety & Compliance, Finance and BIT for more information about tokenization.

c. If the customer wants to store a credit card with the county, have the customer sign the Authorization for Recurring Payments (Included in the Credit Card Standards Manual).

d. Process the credit card transaction as usual. Through the transaction terminal or the payment gateway tokenization platform, enter details about the CCD. Document in a database the token returned from the bank in payment gateway or local spreadsheet regarding the customer. Store the last four digits of the credit card number for reference for the customer in case of refund or account management.

e. For all payments for that customer, use the stored token as a credit card would be used.

f. Deliver receipts to client via preferred method.

E. CCD Storage and Transmission

1. Regardless of how credit card payments are made, the following actions are prohibited:

a. Storing the following CCD in paper or electronic format:

- The full magnetic stripe data or equivalent on a chip

- The personal identification number (PIN) or PIN block

- The 3-digit or 4-digit Security Code value found on the back or front of the credit card

b. Electronically storing the full 16-digit PAN and any CCD, including cardholder name, expiration date and Security Code, along with the PAN. Electronic storage includes, but is not limited to, databases, spreadsheets, documents, scanned images, tweets, voicemails, voice recordings, received emails, sent emails, and email attachments. Only the credit card type and last four or first six digits of the PAN may be stored electronically.

c. Storing credit card information on paper

d. CCD must be securely disposed of when no longer needed for reconciliation, business, or legal purposes. In no instance shall this exceed 45 days, and it should be limited whenever possible to only three business days. Secured destruction of paper documents must be via shredding either in-house or with a third-party provider with certificate of disposal.

G. Display and Masking of PAN
The display of PANs must be masked, and the viewing of PANs must be limited to only Authorized Employees, Volunteers or Contractors with a legitimate need. A properly masked number will show only the first six or the last four digits of the PAN or will be substituted by a payment-application-provided Token. (Contact Safety & Compliance, Finance or BIT for more information on the use of Tokens.) PANs will also be masked in all log repositories, databases, spreadsheets, data stores, removable media, portable digital media, computer screens, credit card receipts, faxes, and paper reports.

H. Mobile Devices (smartphones, tablets, laptops) Used for Credit Card Transactions

1. Conduct mobile transactions only on devices owned and managed by Jefferson County.

2. Use only Point-to-Point Encryption (P2PE or E2EE) solutions that have been approved by Safety & Compliance and BIT to accept credit card payments through mobile devices.

3. Avoid use of mobile applications allowing keyboard entry of CCD. If required, use only mobile applications that have been approved by Safety & Compliance and BIT.

4. Ensure that any mobile device used for transactions is not “rooted” or “jail broken.”

5. Ensure that any mobile device used for transactions is running the latest version of the operating system.

6. Ensure that any mobile device used for transactions is managed by the county’s mobile device management software. Contact Safety & Compliance and IT staff supporting your Department/Division or Elected/Appointed Office for more information.

7. Require any mobile device used for transactions to be locked with a secure PIN.

8. Enable encryption on all mobile devices used to process CCD. Check the help pages for your mobile device vendor or contact your BIT support staff for instructions about how to enable encryption. Do not store credit card data on any mobile device.

9. Mobile devices used for credit card transactions should be locked in a secure location when not in use.

I. Credit Card Technology Inventory and Inspection

1. All personnel working in the CDE must receive training in order to be made aware of attempted tampering or replacement of devices.

2. Conduct a weekly review the Credit Card Technology Inventory Form (Included in the Credit Card Security Manual) weekly and inform BIT of any changes.

3. Ensure that the Credit Card Technology Inventory Form includes all devices used for processing credit cards. The list must include accurate information on the make and model of the devices, the location of the devices (i.e., the building/office location), and the serial number or other unique ID on the device.

4. Perform weekly inspections of credit card processing devices to look for tampering and substitution. Ensure that all device surfaces are inspected for missing or extra cables, differently colored casing, etc. that could be the result of tampering. If any anomalies are discovered, immediately report them to BIT.

5. Verify that no devices are connected to the Jefferson County managed wireless networks.

6. Verify that terminals, PCs, and any other wired credit card processing devices are plugged into only network jacks identified as “CC” or have a distinctive black color.

7. Review any Jefferson County web sites accepting credit card payments and ensure that links to the credit card processing vendor are correct. If any anomalies are discovered, immediately report them to Safety & Compliance and BIT.

J. Visitor Logs

1. Utilize a visitor log with appropriate visitor badges in all areas where PCI workstations, credit card swipe devices, reports, and media can be accessed.

2. Require that visitor badges be clearly displayed and clearly identifiable.

3. Ensure that visitors do not access the CDE unattended or without a business reason.

4. Ensure that visitors surrender their badges before leaving the area.

5. Retain visitor log records for at least three months, and ensure they are kept secure (locked up at night).

K. Remote Access

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

2. Immediately notify 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.

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

L. Computer Security

1. Departments/Divisions and Elected/Appointed Officials shall not develop or purchase software that processes CCD on Jefferson County information technology resources without the approval of BIT.

2. All Authorized Employee, Volunteer or Contractors working in the CDE must have a unique username and password.

3. All computers and applications must prompt for a password in order to log on. Passwords and screensavers must comply with current standards and procedures.

4. IT staff and employees must not disclose private IP addresses and routing information to external entities without explicit authorization from BIT.

M. Physical Security for the CDE

1. Ensure that credit card readers, desktop/laptop workstations and other computer equipment used for handling credit card information are locked in a secure area, or are not easily accessible to visitors, especially after business hours.

2. If you do not have a lockable area such as a desk, closet, or room away from any visitors, an alternative will need to be proposed to the IT staff supporting your Department/Division or Elected/Appointed Office or Safety & Compliance or BIT.

3. Conduct physical security reviews of your Department/Division or Elected/Appointed Office's credit card processing at least monthly, and document the review in the Credit Card Physical Security Review Log (Form is included in the Credit Card Security Manual.) Immediately report any incidents, strangeness, or anomalies to the Safety & Compliance staff supporting your Department/Division or Elected/Appointed Office or Safety & Compliance immediately.

4. Review locked locations where physical credit card numbers are stored on a weekly basis to ensure that no forms have been missed or gone unprocessed.

5. Appropriate facility entry controls must be used to limit and monitor physical access to devices and systems in the CDE.

6. Video cameras and/or access control mechanisms must be used to monitor individual access to those areas that house equipment (e.g. swipe devices, servers, etc.) in the CDE. Contact Safety & Compliance to determine acceptable access control mechanisms.

7. A process must be in place to identify authorized on-site personnel and visitors. Badges or some other highly recognizable feature should be displayed for each person.

8. All visitors must be logged upon entry and departure from the CDE. If you have questions about defining physical boundaries of the CDE for your Department/Division or Elected/Appointed Office, contact Safety & Compliance for assistance.

9. All visitors, whether badged or not, must be escorted in the CDE.

10. All CDE media must be physically secure. This includes computers, removable electronic media, paper receipts, paper reports, and faxes.

11. The security for all CDE storage locations must be reviewed at least annually.

N. Access Control Measures for CCD and the CDE

1. Access to CCD must be restricted by business need to know as determined by the appropriate Department/Division Director or Elected/Appointed Official. Access must be defined according to needs and privilege, job responsibilities, and/or function.

2. Personnel who assign access to CCD and the CDE must be aware of the risk of associating incorrect access to individuals.

3. Access logs must be audited at least quarterly.

4. All access must be documented with the appropriate approval signatures. Initial access will be set to “deny all” and restrictions eased as the job role dictates.

5. All personnel operating within the CDE must be aware of the access control measures.

6. CDE identity and access management procedures must be clearly documented and followed. All users will be assigned a unique user ID and password. All user accounts must be validated against a known and authorized user.

7. CDE access must be revoked immediately if an employee leaves the county, their role no longer requires access, or if any malicious or unnecessary action by a user has taken place.

8. Require that all computers and applications prompt for a password in order to log on, and that the passwords and screensavers comply with current standards and procedures.

9. At no time will group, shared, or generic IDs and passwords be used. Service provider employees with remote access to the CDE (e.g., for support of point-of-sale systems or servers) must use a unique authentication credential such as a password/phrase for each customer.

10. Managers of each Department/Division or Elected/Appointed Office accepting credit card payments must ensure that a copy of the written agreement with their credit card process vendor is stored within their Credit Card Standards Manual.

11. Unless a written exception is documented, all Department/Division or Elected/Appointed Office must have a copy of their vendor's service provider Attestation of Compliance (AOC) in their Credit Card Security Manual.

12. Monitor and review AOC and associated agreements/contracts at least annually.

O. Security Awareness

1. The Director or Elected/Appointed Official shall require that all employees, volunteers or contractors working in the CDE are trained to be aware of suspicious behavior and to report such events to their manager and/or Safety & Compliance and BIT.

2. All employees must confirm that they will adhere to the following before starting work with PCI or a Department/Division or Elected/Appointed Office that accepts credit card payments:

   a. Verify the identity of anyone claiming to be repair or maintenance personnel.

   b. Do not install, replace, move or disconnect devices without approval from Safety & Compliance and BIT.

   c. Be aware of suspicious behavior around devices and computers used to process CCD.

   d. Report suspicious behavior to their manager and/or Safety & Compliance and BIT.

3. Ensure that personnel at point-of-sale locations have received training and can detect and report attempted tampering or replacement of PCI devices.

P. Requests for Compliance Re-certification or Self-Assessment Questionnaires (SAQ)

1. SAQs will be completed by Safety & 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 & Compliance will establish a procedure for the annual collection and submittal of information to comply with industry requirements.

2. Any requests for re-certification of compliance or submittal of a SAQ should be forwarded to the Director of Safety and Compliance.