Procedure Credit Card Handling and Security for IT staff supporting Departments/Divisions or 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 Department/Division or Elected/Appointed Offices 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 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. Self-Assessment Questionnaire (SAQ): The PCI DSS 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.

B. Applicability

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

2. The Authorized Employees, Volunteer and Contractors with Information Technology roles in Departments/Divisions or Elected/Appointed Offices that handle, process, transmit or store credit card data.

3. Safety and Compliance shall review and update this Procedure at least annually. Each Authorized Employee, Volunteer or Contractor with an Information Technology role 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 and 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 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. 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.

3. 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.

4. 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. CCD Storage and Transmission

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

   a. Storing any CCD, including the following, 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 primary account number (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.

2. CCD must be securely disposed of. Secured destruction of paper documents must be via shredding either in-house or with a third-party provider with certificate of disposal.

E. Display and Masking of Primary Account Numbers (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 the 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.

F. 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 and 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 and 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 your IT staff Safety and Compliance or BIT 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 IT 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.

G. Credit Card Technology Inventory and Inspection

1. Verify that no devices are connected to any Jefferson County managed wireless networks.

2. 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 yellow color.

3. 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 and Compliance and BIT.

H. Visitor Logs

1. Utilize a visitor log with appropriate visitor badges in all departmental areas where PCI workstations, credit card swipe devices, reports, and media can be accessed. This includes access to data centers or other areas where CCD may be stored or transmitted unencrypted.

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

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).

I. Wireless Networks and Rogue Access Points

1. On a quarterly basis, perform an inspection of the CDE to ensure that no undocumented network devices, including but not limited to wireless access points and routers, exist within the area.

2. Note date, time, and person performing the inspection.

3. If undocumented network devices or unauthorized wireless access points are found in the department, immediately notify Safety and Compliance and BIT.

J. Remote Access

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

2. 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.

3. Remote Access Authorization forms are required to be completed and an acceptable two-factor authentication technology must be implemented before remote access can be granted.

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

5. Access to systems and networks shall be only on a "need-to-know" bases with access limited to only that needed to perform their job function (Principle of Least Privilege).

K. 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 Safety and Compliance and 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. If a user requests a reset of an authentication credential by phone, email, or other non-face-to-face method, IT administrators must verify the user's identity before modifying those credentials.

5. CCD transmitted over open, public networks must be safeguarded through the use of strong cryptography and security protocols (e.g., TLS 1.2 or higher, IPSec, SSH, etc.). All protocols must only support secure versions and configurations.

6. Servers storing or processing CCD must be configured with only one primary function per server to prevent functions that require different security levels from coexisting on the same server.

7. Wireless networks transmitting CCD or connecting to the CDE must use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission.

8. Wireless networks transmitting CCD or connecting to the CDE must not use default community strings or default passwords on access points.

9. Employees must not disclose private IP addresses and routing information to external entities without explicit authorization from Safety and Compliance and BIT.

10. Software applications, including public-facing Web applications, may not be developed within the CDE.

11. IT staff should conduct periodic network scans to ensure that CCD storage policies have not been violated.

12. Encryption/decryption keys must not be stored within the CDE.

13. Verify that the network setup currently in use matches the documented architecture and standards.

L. Physical Security for the CDE

1. Conduct physical security reviews of your division/department/office's CDE at least monthly and document the review in the Credit Card Physical Security Review Log (Included in the Credit Card Security Manual.) Report any incidents, strangeness, or anomalies to your IT staff or BIT immediately.

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

3. 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 and Compliance and BIT to determine acceptable access control mechanisms.

4. Physical network jacks or ports not in use must be set to "shutdown."

5. 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.

6. All visitors must be logged upon entry and departure from the CDE.

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

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

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

M. 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. Inactive user accounts must be removed/disabled at least every 90 days.

9. Vendor, support or maintenance access user accounts will only be enabled during the time period needed and disabled when not in use. Such accounts will be monitored during use.

10. A lockout mechanism must be triggered after six unsuccessful access attempts. The lockout durations must be set to a minimum of 30 minutes or until an administrator enables the user ID.
11. 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.

12. Passwords must be changed from vendor-supplied default credentials (e.g., a username of “username” or a password of “password”).

13. Passwords will be set administratively for first-time use and changed immediately after the first use.

14. Two-factor authentication must be used for remote network access originating from outside of the Jefferson County networks. This includes Authorized Employees, Volunteers, or Contractors and all third parties (including vendor access for support and maintenance).

15. 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.

16. If other services, protocols, or daemons are considered by Jefferson County to be insecure, then additional security measures will be implemented as deemed appropriate by systems administrators.

N. Network Scanning/Security and Penetration Testing of the CDE

1. Qualified personnel in IT for all Departments/Divisions and Elected/Appointed Offices must perform quarterly internal network vulnerability scan for all networks managed by them. Contact BIT for tools and assistance.

2. Re-scans must be executed immediately after remediation of critical vulnerabilities has occurred and until the scan shows clean results containing no critical vulnerabilities.

3. BIT will ensure that an external network vulnerability scan is performed quarterly by an Approved Scanning Vendor (ASV), and coordinate with all Departments, Divisions and Elected/Appointed Officials to remediate any noted deficiencies.

4. Internal and external scanning must be performed as needed after significant changes to any county networks.

5. Processes must exist to test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points in the CDE on a quarterly basis.

6. If wireless LAN (WLAN) cards are utilized on devices or systems components in the CDE and are not being utilized for a CDE purpose, the cards must be rendered unusable.

7. Computers in the CDE must be examined for attached/portable/mobile devices that can be used to create a wireless access point. If found, the devices must be removed immediately.

8. IT staff must maintain a list of approved wireless access points in the CDE.

9. Incident response procedures must be implemented in the event that unauthorized wireless access points are detected.

10. Mandated penetration tests against the entire CDE and critical systems must be conducted.

    a. External penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification.

    b. Internal penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification.

    c. If segmentation is used to isolate the CDE from other networks, penetration testing must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and all out-of-scope systems must be isolated from in-scope systems.

    d. Any noted deficiencies must be corrected.

11. Penetration testing must be based on an industry-accepted penetration testing approach (e.g., NIST 800-115) and include the following:

    a. Coverage for the CDE perimeter and critical systems

    b. Testing from both inside and outside the network

    c. Testing to validate any segmentation and scope-reduction controls

    d. Review and consideration of threats and vulnerabilities experienced in the last 12 months

    e. Retention of penetration testing results and remediation activities results

12. Application-layer penetration tests must include injection flaws, buffer overflow, insecure cryptographic storage and communications, improper error handling, cross-site scripting, improper access control, cross-site request forgery and other high vulnerabilities identified using current industry best practices.

13. Network-layer penetration tests must include components that support network functions as well as operating systems.

O. Vulnerability Management Program for the CDE

1. Antivirus (A/V) software must be deployed on all systems commonly affected by malicious software such as personal computers and servers.

2. A/V programs must be capable of detecting, removing, and protecting against all known types of malicious software. The A/V software version must be current and updated, and it must perform periodic scans and have the ability to generate audit logs.

3. A/V mechanisms must be actively running and must not be able to be disabled by users unless specifically authorized by management on a case-by-case basis for a limited time period.

4. All vendor security vulnerabilities must be monitored through security mailing lists or direct subscription to vendor information lists or use of reputable outside sources for security vulnerability information. Any newly discovered security vulnerabilities must be assigned a risk ranking of critical, high, medium, or low and remediated appropriately.

5. All vendor-supplied applications/software must be supplied with security patches. Critical or emergency security patches must be installed within one month of release, and all other security patches must be installed within three months.

6. Internal and external network vulnerability scans must be performed at least quarterly and after any significant change to the network.

P. Configuration Management for the CDE

1. A current baseline configuration of all firewall and router devices that control computer traffic to and within the CDE must be maintained, as well as an inventory of each system's constituent components and relevant ownership information.

2. Firewall and router rule sets must be reviewed at least every six months, and reviews must be documented to verify that they are occurring.

3. Changes to each firewall and router must be documented and controlled, and changes must be approved in accordance with each division/department/office's Change Control Management process.

4. All Jefferson County baseline system configurations must be retained for the in-service lifetime of the system plus two years.

5. Changes to each information system must be monitored, and security impact analyses must be conducted to determine the effects of the changes.

6. Physical and logical access restrictions associated with changes to each information system must be enforced, and records reflecting all such changes must be generated, retained, and reviewed.

7. Mandatory configuration settings for information technology products must be established within the information system, the security settings of information technology products must be configured to the most restrictive mode consistent with operational requirements, the configuration settings must be documented, and the configuration settings must be enforced in all components of the information system.

8. All configuration items must be put under configuration management prior to a production release.

Q. Intrusion Detection and/or Intrusion Prevention for the CDE

1. All network devices and equipment will be configured such that access to the devices within the CDE is logged. Security alerts must be generated by perceived intrusions against a known network signature and monitored 24/7 so that the attempted intrusion can be stopped.

2. All access to CCD and network resources in the CDE must be tracked and monitored.

3. Audit trails must be used to link all access to system components to each individual user.

4. All individual access to CCD must be logged.

5. All actions taken by any Authorized Employee, Volunteer or Contractor with root or administrative privileges must be logged. Any unauthorized access should be immediately reported to Safety and Compliance and BIT.

6. Logging must be enabled for invalid logical access attempts.

7. Logs for external-facing technologies must be written onto a secure, centralized internal server or media device.

8. File-integrity monitoring or change-detection software must be used on logs to ensure that existing log data cannot be changed without generating an alert.

9. The following must be reviewed at least daily: all security events, logs of all system components, logs of critical systems components, and logs of all servers and system components that perform a security function (firewalls, IDS/IPS, authentication servers, etc.).

10. Follow-ups on all anomalies and/or exceptions must be carried out in an expeditious manner.

11. Audit trail histories must be retained for at least one year.

R. Security Awareness

1. The Director or Elected/Appointed Official of IT staff handling, storing or transmitting CCD shall require that all employee, 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 the Safety and Compliance and BIT.

2. All personnel must confirm that they will adhere to the following before starting work in 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 permanently disconnect credit card devices without approval from Safety and 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 and Compliance and BIT.

S. Antivirus/Anti-Spyware

1. Ensure that all desktop computers and laptops have some type of antivirus software installed on them. Perform periodic checks to ensure the following:

a. The antivirus software is set up to perform complete system scans on all computers periodically.

b. The antivirus software is set up to receive automatic updates for its virus definitions.

c. The antivirus software scans all email attachments and Internet downloads.

2. Antivirus software is current and operating correctly.

T. Requests for Compliance Re-certification or Self Assessment Questionnaires

1. 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.

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