Title: Administrative Policy Credit Card Payments	**Policy No.** Part 4, Financial Administration Chapter 8, Credit Card Payments Section 1
	Effective Date December 11, 2018
Policy Custodian Finance & Safety and Compliance	**Adoption/Revision Date** December 11, 2018/December 2019

Adopting Resolution(s): CC18-412

References (Statutes/Resos/Policies): 29-11.5-103 CRS, CC08-263, CC15-379, CC15-447

Purpose: To provide for the security of Jefferson County's credit card data, protect against data exposure and possible theft, comply with credit card industry requirements, and minimize the costs/fees incurred by the County as a result of offering alternative payment methods.

Policy:

A. Definitions

1. 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.

2. 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.

3. 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.

3. 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. The standard was created to increase controls around cardholder data and to reduce credit card fraud via exposure of that data.

B. Applicability

1. This Policy shall apply to all Departments/Divisions that report to the Board of County Commissioners, Elected Officials Offices and Appointed Officials Offices.

2. The Business Innovation and Technology Division (BIT) and Finance Divisions may create and maintain procedures, standards, and other documents to ensure compliance with PCI DSS, vendor requirements, and other measures deemed

necessary to protect CCD and the CDE. Some County Departments/Offices may impose additional procedures, standards and governing the use and protection of CCD and the CDE.

3. Employees, volunteers and contractors who handle or process CCD or work in the CDE will be required to confirm that they have read, understand and agree to abide by this Policy, and any applicable procedures, standards, and/or other documents. Acknowledgements will be required annually.

4. Employees volunteers and contractors who handle or process CCD or work in the CDE will be required to undergo training related to the use and protection of the CCD and the CDE of a type and frequency as prescribed by the applicable Department of Office or the BIT.

C. Credit Card Processing

1. The County will use third party vendors for transaction processing. Procedures for Credit Card Processing Vendor Evaluation, Contracting and Management will be followed when selecting third party vendors.

2. The County may collect a transaction fee on credit card purchases. The amount collected shall not exceed the actual cost incurred by the County to process the transaction by credit card. The County prefers the use of vendors that collect the transaction fee as part of their service fee. In the event that the credit card vendor collects the transaction fee from the customer at the time of transaction, the County will not collect an additional transaction fee.

D. Compliance with Industry Standards

1. Approvals

a. The Safety and Compliance Director and the Finance Director must approve all credit card processing proposals as a condition to the County entering into any contract, purchasing credit card processing services or equipment, adding merchant accounts, or installing, moving or disconnecting any credit card devices. Approvals are required, regardless of the transaction method, such as online processing, swipe terminals, desktop/laptop computers or mobile devices and whether wired or wireless.

b. The County Attorney's Office must approve all contracts for credit card processing services and devices.

c. Only authorized employees, volunteers, or contractors shall handle or process CCD or work in the CDE. Human Resources and the appropriate Department/Division Director or Elected/Appointed Official shall confirm that a thorough background check for individuals handling or processing CCD or operating in the CDE has been conducted, prior to hiring, contracting, or assignment.

2. Inventory
   BIT shall maintain an inventory of all web portals, swipe readers, mobile device apps/readers, cash registers and any other services or devices used to process or store CCD. The inventory shall include information about the type of device/service including, but not limited to: processing vendor, merchant ID, Jeffco website URL, device manufacturer/model/serial number, physical location and all county authorized employees, volunteers, and contractors that handle or process CCD or work in the CDE.

3. Assessments

   a. The Safety and Compliance Director and the Finance Director shall develop and update a Credit Card Standards Manual that will be readily available to all employees, volunteers or contractors. The appropriate Department/Division Director or Elected/Appointed Official shall ensure that all employees, volunteers and contractors who handle or process CCD or work in the CDE are familiar with and adhere to this Policy, the Credit Card Standards Manual and any applicable procedures, standards, and other documents to ensure compliance with PCI DSS.

   b. The Safety and Compliance Director shall conduct periodic assessments of the county's compliance (including volunteer and contractor compliance) with industry, vendor and county policies, the Credit Card Standards Manual and any applicable procedures, standards, and other documents related to the handling of or processing of CCD or operating in the CDE, initiate actions to remediate any non-compliance issues, and submit appropriate compliance documentation to vendors. Department/Divisions or Elected/Appointed Official's Offices that are found to be out of compliance with PCI DSS standards shall work with the Safety and Compliance Director, BIT and their own Information Technology staff, if applicable, to remediate all compliance issues in a timely manner so as to avoid audit findings and fines.

   c. BIT is the only organization authorized to submit a "Self-Assessment Questionnaire" (SAQ) to a credit card processing vendor or industry association on behalf of the county. BIT shall establish a procedure for the annual collection and submittal of information to comply with vendor and industry requirements.