	Rockingham County Policies & Procedures **CREDIT CARD POLICY**		
Department: Information Technology		**Effective Date: 09/05/19**	**Pages:** 4
Prepared By: Derek Southern, CIO		**Revised by/date:**	
Approved By: Board of County Commissioners			
Authority Source: Board of County Commissioners			

1.1 PURPOSE

The purpose of this policy is to establish business processes and procedures for accepting payment cards at participating Rockingham County offices. This will minimize risk and provide the greatest value, security of data, and availability of services to each participating County unit and its citizens. This policy follows all rules and regulations established by the Payment Card Industry (PCI) and articulated in the PCI Data Security Standards (DSS). Additionally, these processes are intended to ensure that payment card acceptance procedures are appropriately integrated with the County's financial and other systems.

For the purpose of this policy, use of the term "credit cards" shall include the acceptance of cards bearing the credit card company logo of Visa, MasterCard, or Discover. Only those units which have received approval will be permitted to accept credit cards for payment of goods or services. The ability to accept credit cards comes with significant responsibilities to maintain cardholder security and to mitigate the risk of fraud. Rockingham County, and all of its comprised offices and units, have a fiduciary responsibility to protect citizen credit card information, and thus must adhere to the strict security requirements established by PCI DSS or face significant financial penalties if a breach or fraud occurs. It is also noteworthy that any compromise of cardholder information undermines public confidence in the County's ability to maintain appropriate stewardship over entrusted confidential information. Lack of compliance in a single area of the County could jeopardize the County's ability as a whole to accept payment cards.

2.1 DEFINITIONS

Cardholder
The customer to whom a payment card has been issued or the individual authorized to use the card.

Encryption
The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.

Merchant or Merchant Department
For the purposes of the PCI DSS and this policy, a merchant is defined as any County department or other entity that accepts payment cards bearing the following logos Discover, MasterCard or VISA as payment for goods and/or services, or to accept donations.

Payment Card
Any payment card/device that bears the logo of Discover Financial Services, MasterCard Worldwide, or VISA, Inc.

Payment Card Account Change
Any change in the payment account including, but not limited to:

- the use of existing payment card accounts for new purposes;
- the alternation of business processes that involve payment card processing activities;
- the addition or alteration of payment systems;
- the addition or alteration of relationships with third-party payment card service providers and
- the addition or alteration of payment card processing technologies or acceptance channels.

Payment Card Industry (PCI) Data Security Standard (DSS)
A multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Personal Identifiable Information (PII)
All personally identifiable data about the cardholder such as:

- Cardholder Name
- Credit Card Number
- Cardholder Verification Value (CVV2) – the 3 or 4 digit code located on the back of the credit card
- Address
- Magnetic Stripe Information

3.1 POLICY

1) County personnel who receive or process credit card information must properly safeguard this sensitive information. This policy applies to all County personnel who receive Personal Identifiable Information (PII) while processing, retaining/storing and disposing credit card data.
   a) Only trained County personnel are permitted to handle PII data. Interns or untrained employees are only permitted to handle PII at the discretion of the department and with additional training and certification of knowledge of the policy. Such staff will not be given access to PII data that is stored.
   b) Any employees that are permitted to handle credit card transactions will be subject to a criminal and credit background check. These background checks will be performed by the Human Resources department.. Any questionable items will be reviewed by the County Attorney for final decision.
   c) Employees with access to credit card information are held accountable to the Rockingham County Privacy policy.

2) All third party vendors software/systems used to process credit/debit card transactions must be compliant with the Payment Card Industry (PCI) Data Security Standards.

3) County Departments wanting to accept credit card payments must contact Financial Department to determine the best way to allow for their acceptance. In some instances, training on the policies and proper procedure may apply.

4) Any suspected loss or theft of materials containing PII data must be reported the employees immediate supervisor if they suspect a violation or by contacting the Finance Department.

5) Departments must not retain any credit card information. All credit card and PII submitted on a refund form will be maintained in the Finance Department. Once processed, any forms that must be retained for audit purposes that include credit card information must have the card number and expiration date rendered unreadable.

6) For departments with approval to process credit cards and retain PII within their department:
- **a)** Credit card terminals must be settled at the close of business each day. Online credit card transactions are settled automatically at the designated time.
- **b)** Reconciliations between the settlement reports and bank deposits will be performed by the Finance Department.
- **c)** The Finance Department will handle any 'chargebacks' or disputes within the stated deadlines. Supporting documentation from the department originating the charge must be provided (if needed) within the deadline.
- **d)** PII data must never be released without a legitimate business requirement and requires Finance Director and County Attorney approval.
- **e)** Only the last 4 digits of the credit card are to be displayed on a receipt.
- **f)** County Employees will never retain the three or four digit validation code (CVV2) or magnetic stripe information, in any form.
- **g)** Access to PII data must be restricted and all data must be safeguarded from fire and theft. PII data must be stored in a secured, access controlled area in a locked container to prevent unintentional or malicious compromise.
- **h)** All PII must be shredded 12 months after the transaction was processed.
- **i)** When merchant services processors or card associations make significant policy or procedural changes, Finance will notify the departments.

3.2 PROCEDURES

1) All credit card payments received and/or processed by the departments must be supported by appropriate documentation as stated below:
- **a)** All in-person payments must be supported by the signed copy of the receipt produced by the secure website.
- **b)** All payments received through telephone request must have the designated form attached to the County's receipt. The customer copy of the receipt may be emailed at the request of the individual.
- **c)** The Finance office has limited access to processing payments to ensure segregation of duties.

2) As required by PCI standard, offices processing credit card transactions and maintaining PII must have written procedures that include the following:
- **a)** Segregation of duties
  - **i)** In most situations initiating transactions, the daily deposit and the reconciliation to the bank are done by different individuals.
  - **ii)** Roles and responsibilities of each department employee are determined and overseen by the department head or supervisor.
- **b)** Deposits
  - **i)** Money is deposited the next working day from when it is processed in the payment system.
  - **ii)** The individual balancing reports are combined into a daily deposit report. Receipts are verified. Credit card payments should match the amounts of the settlement reports. Any discrepancies are noted and corrected as soon as possible.
- **c)** Reconciliation procedure
  - **i)** Bank reconciliation is done on a daily basis, using the deposit report, which includes all credit card transactions.
- **d)** Physical Security
  - **i)** All credit card information processed by the receiving department/office is stored in a secured file room or space.
  - **ii)** The files or space is to remain locked at all times and access is restricted.

4.1 WHO SHOULD KNOW THIS POLICY

Any individual with responsibilities for managing credit card transactions and those employees entrusted with handling or processing credit card information. This includes budget officers and systems managers and all Rockingham County employees, contractors, consultants or agents who, in the course of doing business on behalf of the County, accept, process, transmit, or otherwise handle cardholder information in physical or electronic format.

This policy applies to all County departments and/or agents that accept credit card payments.