9. CREDIT CARD AND CHECK ACCEPTANCE POLICY

GENERAL POLICY

The establishment of control measures for credit card transactions is necessary to maintain proper security over credit cardholder information. The purpose of this policy is to establish guidelines for processing charges/credits on credit cards to protect against exposure and possible theft of account and personal card holder information and to comply with the Payment Card Industry's Data Security Standards (PCI DSS) requirements for transferring, handling and storage of credit card information.

SCOPE

This policy is applicable to all offices and departments within Scott County government.

PURPOSE

The County has adopted the following policy and departmental procedures for all types of credit card activity transacted in-person, via fax, mail or Internet. Any department utilizing a web based storefront must use due diligence to choose a vendor that can provide a secure environment. Individual departments may determine if it is necessary or feasible to accept payments via credit/debit cards by considering the volume and frequency of payments received.

SPECIFIC POLICY PROVISIONS

Types of Cards Accepted

Departments may only accept merchant cards from credit card associations that have agreements with the vendor utilized by the County.

Transaction or convenience fees

Transaction fees (convenience fees) shall be charged to cover the cost of permitting a person to complete a transaction using a web application or other means of electronic access. The Conservation Board may enact rules or regulations related to the acceptance of credit cards for recreation transactions.

Any revenues from transaction fees and expenditures funded by the fee must be accounted for separately to provide an audit trail on the collection and use of the fees.

Responsibility of Departments

A Department shall consider the following items before deciding to accept credit cards:

1) Determine the volume of transactions handled annually to determine the business need for accepting credit cards.
2) Ensure that all credit card data collected, regardless of how it is stored (physically or electronically, including but not limited to account numbers) is secured. Ensure that only secure communication protocols and/or encrypted connections are being utilized for processing electronic transactions.
3) Ensure access to credit card data is limited by business need-to-know and that employees have a unique ID for computer access to this data.
4) Ensure that any contract with a vendor to conduct credit card transactions complies with County Policy 17 Identity Theft Prevention Program.
5) Ensure employees are familiar with County Policy 17 Identity Theft Prevention Program and trained biennially on the issues. Ensure that applicable employees are trained on merchant card rules.
6) Departments shall consult with the Webmaster to create a "store front" on the County's web site to ensure continuity and comfort in the individual that the transaction is being conducted with the County on a secure site.

Business Functions

Employees accepting credit cards shall:

1) Credit card transaction shall only be performed by authorized staff.
2) If the employee handles the credit card during a transaction, the signature must be verified with the signature on the card or a picture ID observed.
3) No phone transactions (i.e. card not present) shall be allowed.
4) An authorization approval code must be obtained from the merchant card processor, with real time authorization being the preferred method or telephone authorization as an alternative.
5) If authorization is not received the card cannot be accepted and an alternative payment means of payment will be required.
6) If fraud is suspected the procedures in County Policy 17 Identity Theft Prevention Program shall be followed.
7) Refunds or credits are to be pre-approved by management. They are to be processed to the original credit card number charged. Any exceptions are to be made by the Department Head. Refunds and credits are allowed under a reasonable time period established in advance by the department.
8) Departments may have more specific processes for accepting credit cards.
9) It is highly recommended that departments and offices utilize the same processor as the Treasurer.

Regular Process and Reports

Reconciliation shall be done by the department on a daily basis, and all credit card information will be handed over to the Treasurer's office with the same frequency as any cash collected. Departments shall establish written procedures related to daily processes for reconciliation.

Chargebacks will be handled by the department responsible for the charge.

Departments shall receive training on how to journalize transactions from Treasurer's Office.

Confidentiality and Security of Account Information

In order to maintain confidentiality of data the following processes must be followed:

1) Any hardcopy containing cardholder information will be destroyed immediately after processing. Credit card information shall not be stored for future use such as periodic billing or partial payments.
2) Only the last four digits of any credit card shall appear on a receipt or document where credit card information is displayed.
3) Any electronic media containing cardholder information shall be securely collected and held as confidential. The County shall not store credit card account numbers.
4) The three digit card validation code printed on the signature panel of a credit card is never to be stored in any form.
5) Employee shall not obtain or transmit credit card information via e-mail.
6) All transactions shall occur at workstations that have antivirus software installed and updated regularly.
7) Terminals shall be located in secure area during and after work hours to prevent unauthorized access. Employees shall ensure logging off at the conclusion of the workday.
8) Background checks shall be performed prior to hiring or promoting any position with unrestricted access to credit cardholder information.

Process for responding to a Security Breach

In the event of a security breach or suspected security breach the Department must do the following:

1) Comply with County Policy 17 Identity Theft Prevention Program
2) Contact the IT Director to assure the preservation of any electronic evidence and remediation.
3) Alert the merchant bank, payment card association and Sheriff's office. The Department Head will notify the County Administrator who will in turn notify the appropriate officials of any suspected breaches.
4) Within 48 hours of the breach the Department Head will provide the affected credit card association with proof of PCI compliance.
5) Within 4 business days of the breach the Department Head will provide the affected credit card association with an incident report.
6) At the request of the credit card association or depending on the level of risk and data elements compromised the IT Director will arrange for a network system vulnerability scan.
7) In the event that personal data is exposed the department shall comply with County Policy 17 Identity Theft Prevention Program.

Acceptances of checks

Before accepting check payments the department shall post signage indicating that all checks will be converted into ACH transactions and will processed electronically. In addition, the receipt shall provide written notice of this disclosure.

A service charge of $30 will be imposed for each check, ACH payment, or other draft tendered which is subsequently dishonored or otherwise refused by the bank or other payer. Acceptance of any check or other draft shall be only upon this condition, to which the person tendering the check or draft is deemed to have consented.

Additional resources:
Payment Card Industry Data Security Standard:
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
Visa Merchants Cardholder Information Security Program:
http://usa.visa.com/merchants/risk_management/cisp_overview.html
Mastercard International Rules Manual:
http://www.mastercard.com/us/merchant/support/rules.html