TITLE 10

SPECIAL ORDINANCES, REGULATIONS, RULES, POLICIES, AND BARGAINING AGREEMENTS

SUBTITLE 3 — POLICIES

POLICY 38

Payment Card Security

TABLE OF CONTENTS

38.010 Background

Many Linn County elected officials and departments accept payment by merchant card from individuals for a wide range of services and products. Merchant card transactions are subject to requirements developed by the Payment Card Industry. These requirements are intended to protect information associated with the merchant card and utilized in the processing of merchant card transactions from unauthorized use or disclosure.

[Adopted 2014-008 eff 1/14/2014]

38.015 Policy

It is the policy of Linn County that the processing of merchant card transactions is to be handled in a manner that protects the cardholder information necessary to process the transactions and in compliance with credit and banking industry security standards. Linn County employees will maintain proper financial controls and ensure cardholder information is protected against theft and improper or unauthorized usage and comply with all credit and banking industry security requirements related to the receipt and processing of payment card transactions and any necessary reporting requirements.

[Adopted 2014-008 eff 1/14/2014]

38.020 Applicability

This Policy applies to elected officials, department heads, managers, supervisors, and employees who process, transmit, handle, or store cardholder information or data associated with merchant card transactions in any physical or electronic format.

[Adopted 2014-008 eff 1/14/2014]

38.025 Definitions

(A) As used in this Payment Card Security Policy, unless the context requires otherwise:

(1) **"Acquirer"** means a bankcard association member that initiates and maintains relationships with merchants that accept Visa, MasterCard, or Discover cards. Unless otherwise provided, an "Acquirer" may also be referred to as "acquiring bank" or "acquiring financial institution."

(2) **"Breach"** means an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized individual.

(3) **"Cardholder information"** means any personally identifiable data associated with a cardholder. Examples of cardholder information include, but are not limited to account number, expiration date, card type, name, address, social security number, service code, card validation code, card verification code, personal identification number, and any data from the magnetic strip on the card or contained on a chip or elsewhere and located on the card.

(4) **"Merchant"** means the Linn County office or department that accepts payment cards for payment for goods or services or any fees.

(5) **"Merchant card"** means a card accepted as a method of payment of any amount payable to Linn County with a logo on the face of the card, including but not limited to Visa, MasterCard, or Discover, and may also be called payment card, branded card, credit card, or debit card.

(6) **"Merchant Card Processor"** means the vendor selected by the Treasurer's Office through a competitive selection to process payment cards on behalf of Linn County.

(7) **"Merchant Identification Number"** means a unique number assigned to each terminal location or E-Commerce site that is used to track financial activity or transactions.

(8) **"Payment card"** means a card accepted as a method of payment of any amount payable to Linn County with a logo on the face of the card, including but not limited to Visa, MasterCard, or Discover, and may also be called merchant card, branded card, credit card, or debit card.

(9) **"Payment Card Industry"** means a council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International on September 6, 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

(10) **"Payment Card Industry Data Security Standard (PCI-DSS)"** means the series of requirements for handling, transmitting, processing, and storing cardholder information and includes the PCI-DSS as it may be amended from time to time.

(11) **"PCI Compliance Manager"** means the Linn County Treasurer or designee responsible for developing, implementing, and updating the practices and procedures required to comply with the PCI-DSS and this Policy as well as other duties specified within.

[Adopted 2014-008 eff 1/14/2014]

38.030 General Requirements

(A) The PCI-DSS sets forth twelve requirements for all merchants accepting payment by payment cards as follows:

(1) install and maintain a firewall configuration to protect Cardholder Information;

(2) manage passwords and other security parameters;

(3) protect stored cardholder information;

(4) develop encryption protocols;

(5) install and maintain anti-virus software or programs;

(6) develop and maintain secure systems and applications;

(7) restrict access to cardholder information;

(8) manage unique identification for each person with computer access to cardholder information;

(9) restrict physical access to Cardholder Information;

(10) track and monitor all access to network resources and Cardholder Information;

(11) test security systems and processes; and

(12) maintain a policy that addresses information security.

[Adopted 2014-008 eff 1/14/2014]

38.035 Responsibilities of the Linn County Treasurer's Office

(A) The Treasurer's Office is responsible for overseeing all payment card transactions accepted for payment by Linn County elected officials and departments.

(B) The Linn County Treasurer or designee will be the PCI Compliance Manager for Linn County.

(C) The PCI Compliance Manager is responsible for managing Linn County's PCI-DSS activities, which includes but is not limited to:

(1) developing, implementing, and updating the procedures required by Linn County and the Payment Card Industry;

(2) approving all merchant applications to provide payment card services to the public;

(3) enrolling new merchants and consulting with existing merchants;

(4) coordinating with merchants and the Linn County Information Technology Services (ITS) Department to work through technical requirements that may exist for the secure processing of payment cards;

(5) coordinating Linn County's payment card processor contract and working with Linn County's card processor to obtain merchant identification numbers;

(6) providing training and education on payment card processing and security;

(7) obtaining and retaining a signed Payment Card Merchant Compliance Statement, which includes acknowledgment by the employee that he or she has read and understood this Policy and procedures, from all employees handling cardholder information; and

(8) notifying appropriate parties in the event that cardholder information may be or has been compromised or a suspected breach has occurred and taking immediate steps to work with the payment card acquirer and processor to take appropriate action.

(D) The Treasurer's Office will partner with its sponsoring merchant card processor and payment card acquirer for all payment card transactions accepted for payment to Linn County elected officials and departments.

(E) The Treasurer's Office will ensure that any merchant card processor doing business with Linn County will provide proof of compliance with PCI-DSS at least annually or when any change is made to PCI-DSS or software or hardware used for payment card transactions.

[Adopted 2014-008 eff 1/14/2014]

38.040 Responsibilities of Linn County Elected Officials and Departments

(A) Linn County elected officials and departments interested in accepting payment cards for amounts payable to Linn County must apply for authorization to the Linn County Treasurer's Office by submitting a Merchant Account Application form.

(B) The following steps must be followed in order for any elected official or department to accept payment cards:

(1) Complete and submit the Linn County Application for a Merchant Account to the Treasurer's Office, as well as the internal control policy utilized by the office or department.

(2) The approval of the application by the Linn County Treasurer will be based on the elected official's or department's ability to comply with this Policy and the PCI-DSS.

(3) Upon approval of the application, the Treasurer's Office will coordinate with the payment card provider and obtain the necessary hardware or software to allow the proper configuration of the system to accept payment cards.

(4) Prior to processing payment card transactions, each office or department must arrange for all employees who will handle pay-

ment card transactions to attend a training course provided by the Treasurer's Office. This course must be repeated and confirmed annually.

(5) Once the application is accepted by the Treasurer's Office, the elected official or department becomes a Merchant.

(C) Merchants are responsible for:

(1) ensuring that all practices and processes for accepting, processing, retaining, and disposing of cardholder information comply with PCI-DSS and all other applicable policies and standards;

(2) paying all bank fees associated with their merchant transactions;

(3) paying for all costs of ordering and maintaining the necessary equipment and supplies; and

(4) utilizing only those payment processors and acquirers approved by the Treasurer.

(D) If merchants accept cardholder information via facsimile transmission, the facsimile machine must be located in a secure area with limited access as further described in Section 38.070(F).

(E) Merchants must ensure that all employees that may process, transmit, store, reconcile or otherwise handle payment cards attend payment card training conducted by the Treasurer's Office.

(F) Merchants must ensure that all employees that may process, transmit, store, reconcile or otherwise handle payment cards sign the Payment Card Merchant Compliance Statement to document the employees' understanding of and compliance with this Policy. The original signed Compliance Statement must be sent to the Treasurer's Office, with a copy retained in the employee's departmental file.

(G) Elected officials and departments may not establish their own banking relationship to process payment cards.

[Adopted 2014-008 eff 1/14/2014]

38.045 Internal Controls for Offices and Departments

(A) Offices and departments will develop and maintain operational procedures for each merchant terminal and submit such procedures to the PCI Compliance Manager for review. Operational procedures should address the following areas:

(1) physical security of cardholder information;

(2) disposal of cardholder information;

(3) segregation of duties:

(a) to the extent possible, offices and departments should establish a segregation of duties between payment card processing, the processing of refunds, and financial reconciliation; and

(b) require supervisory approval for any refund transactions;

(4) reconciliation procedures:

(a) all payment card terminals and website applications should be closed out and reconciled at least once each day in accordance with section 38.050; and

(b) a merchant spreadsheet completed and provided to the Treasurer's Office each day the office or department processes payment card transactions.

[Adopted 2014-008 eff 1/14/2014]

38.050 Reconciliation Procedures

(A) In order to reconcile payment card transactions, the following procedures will be followed:

(1) Offices and departments will perform a transaction settlement procedure (close) at the end of each business day. This process electronically sends a payment file to the bank for all transactions received since the previous settlement procedure. A batch settlement report must be produced at this time.

(2) The batch settlement report will be attached to the individual sales receipts and filed in a secure location within an appropriate file within the office or department.

(3) A Treasury Merchant Deposit Spreadsheet must be created and sent electronically to the Treasurer's Office in the format required by that office for every batch that is settled. The spreadsheet must be separate from

the cash and check deposit spreadsheet. Failure to send a Merchant Spreadsheet to the Treasurer's Office that reconciles to the batch report may result in an office's or department's loss of payment card processing privileges.

(4) The Treasurer's Office will match the Merchant Spreadsheet with the bank report and send a receipt back to the office or department that created the Merchant Spreadsheet.

[Adopted 2014-008 eff 1/14/2014]

38.055 Disputes and Chargebacks

(A) In the event of a dispute regarding a payment card transaction by the cardholder, the merchant that handled the payment card transaction must supply documentation substantiating the payment in a timely manner.

(B) If the documentation is insufficient to substantiate the payment card transaction or is not provided in a timely manner and a dispute is filed by the cardholder within two years of the disputed transaction with the issuing bank, the issuing bank will conduct an investigation.

(C) Upon receipt of notice of an investigation into a disputed transaction by the Treasurer's Office from the payment card processor and corresponding sales draft request, the Treasurer's Office will immediately forward the request to the appropriate merchant for response.

(D) The merchant must send the required documentation of the transaction to the payment card processor in accordance with timing requirements set by the payment card processor.

(E) A copy of the materials submitted to the payment card processor must be retained and the date of submission documented.

(F) If the office or department fails to prove the legitimacy of the transaction, the bank will charge back to the merchant the entire value of the transaction, along with an additional fee.

[Adopted 2014-008 eff 1/14/2014]

38.060 Responsibilities of Employees

(A) Linn County employees that may process, transmit, store, reconcile or otherwise handle payment cards must comply with this Policy, all relevant PCI-DSS requirements, attend Payment Card Processing training, and sign the Payment Card Merchant Compliance Statement.

(B) Linn County employees whose duties require the handling of cardholder information should adhere to the following guidelines for acceptance, processing, retention, and disposal of cardholder information:

(1) verify signature of cardholder at the time of the transaction;

(2) verify that the payment card's expiration date is valid;

(3) obtain the signature of the cardholder on the receipt and provide a duplicate copy to the cardholder; and

(4) refuse to accept cardholder information via end-user messaging technologies, which include but are not limited to electronic mail (e-mail), voicemail, instant messaging, and text messaging.

(C) Linn County employees must immediately notify the PCI Compliance Manager and their supervisor upon discovery of a compromise, breach or potential breach in the security of cardholder information.

[Adopted 2014-008 eff 1/14/2014]

38.065 Responsibilities of ITS Department

(A) The Linn County ITS Department is responsible for implementing, and approving, if necessary, all computer networking, computer programming, and information system services necessary for Linn County elected officials and departments to provide payment card services to the public in a manner that is compliant with PCI-DSS.

(B) The ITS Department is responsible for working with the PCI Compliance Manager to meet PCI-DSS requirements related to information systems used by Linn County and providing documentation to the PCI Compliance Manager as necessary.

[Adopted 2014-008 eff 1/14/2014]

38.070 Security and Retention of Cardholder Information

(A) Linn County will comply with all PCI-DSS to ensure the safekeeping and proper destruction of cardholder information.

(B) It is the responsibility of the office or department to follow Linn County's payment card policy and procedures to ensure payment card transactions are processed safely.

(C) All offices and departments authorized to accept payment cards must:

(1) exercise reasonable care in screening transactions to reduce payment card misuse and loss of funds;

(2) establish and maintain a proper security environment to safeguard an individual's payment information at all times;

(3) process payment card transactions using approved electronic data capture machines received from the Treasurer's Office;

(4) conduct payment card transactions in person, by telephone, by mail, or via secure and pre-approved internet application;

(5) never send or accept cardholder information or payment card information via electronic mail; and

(6) never store sensitive authentication data, including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks used to authenticate cardholders or authorize payment card transactions subsequent to authorization.

(D) The following practices and procedures must be followed by Merchants that accept payment card transactions:

(1) Merchants will not store, process, or transmit cardholder information on Linn County's network.

(2) Merchants will never transmit cardholder information by end-user messaging, such as telephonic text messages, e-mail, instant messaging or chat.

(3) Merchants will not create an electronic file, such as a word processing document, spread-sheet, database, or image containing cardholder information.

(4) If internet transactions are conducted, files received from the acquiring bank must not contain any cardholder information other than the name of the individual conducting the transaction with the merchant.

(5) Merchants will never store cardholder information on portable devices, including laptops, external hard drives, or flash drives.

(E) Cardholder information shall not be retained or stored electronically or in paper format, unless the cardholder information is necessary for business purposes and:

(1) the transaction is conducted by mail; or

(2) the payment card processing device is not available for immediate processing.

(F) In the event one of the two exceptions in the above subsection LCP 38.070(E) is met:

(1) cardholder information necessary to process the payment card transaction must be received in paper form and must be kept in a secure location as required by this Policy; and

(2) payments for which cardholder information is retained in paper format must be processed within two business days of receipt and immediately after processing the paper form containing the cardholder information must be disposed of by cross-cut shredding or placement in a locked confidential shredding bin.

(G) Procedures must be created to appropriately secure any paper that contains sensitive cardholder information; if cardholder information does need to be physically retained for business purposes, then the following practices and procedures must be followed:

(1) All materials, including hard copy media, containing cardholder information must be made physically secure and retained, stored, or archived only within secure Linn County office environments.

(2) Within secure Linn County office environments, all materials, including hard copy media, must be stored in a secure and locked container, such as a locker, cabinet, desk, safe, or other similar secure container and clearly disting-

uishable as "confidential" through labeling or other method.

(3) If paper records containing payment card account numbers are stored, all but the last four digits must be redacted within 60 days, or as soon as refunds or disputes are no longer likely, but in no case later than 180 days after the transaction.

(4) Access to sales drafts, reports, or other sources of cardholder information must be limited to employees with a need-to-know basis.

(5) Printed receipts of payment card transactions that are distributed outside of the office or department of the merchant accepting the payment card transaction must show only the last four digits of the payment card number.

(6) At no time is printed material or hoard copy media containing cardholder information to be removed from any Linn County office or secured storage area without prior written authorization from management.

(7) Distribution of confidential or sensitive hard copy media containing cardholder information must be sent or delivered by a secured courier or other delivery method that can be accurately tracked at all times.

(8) Custodians of hard copy material containing cardholder information must perform an inventory of the media at least annually, with the results of such inventories being recorded in an inventory log.

[Adopted 2014-008 eff 1/14/2014]

38.075 Disposal of Material Containing Cardholder Information

(A) All materials and media containing cardholder information must be destroyed after the minimum time deemed necessary for its use has passed or when it is no longer needed for business or legal reasons.

(B) All materials and media containing cardholder information must be rendered unreadable prior to discarding the material.

(C) Hard copy media and other materials must be destroyed by cross-cut shredding, incineration, or pulping so that cardholder information cannot be reconstructed.

[Adopted 2014-008 eff 1/14/2014]

38.080 Breach Notification

(A) If at any time a Linn County employee experiences or discovers a breach or potential breach or compromise of ay payment card information or related data, that employee must report the event immediately to the PCI Compliance Manager.

(B) The PCI Compliance Manager will assess the situation and contact the appropriate merchant services partners and acquirers and begin an evaluation to determine the appropriate level of response.

[Adopted 2014-008 eff 1/14/2014]

38.085 Fees

(A) Each payment card transaction is assessed a variety of fees, with the fees accumulating for each merchant identification number.

(B) Merchants will be responsible for the actual costs incurred to process payment card transactions, including setup, monthly fees, and hardware and software costs, when applicable.

(C) The above described fees are charged back to the responsible merchant on a monthly basis by the Treasurer's Office.

[Adopted 2014-008 eff 1/14/2014]

38.090 Prohibited Activities

(A) Linn County officials and employees handling payment card transactions are prohibited from doing the following activities:

(1) providing cash advances to payment card holders;

(2) processing an amount that exceeds the amount payable to Linn County or any other "cash back" scheme;

(3) adjusting the amount payable to Linn County based upon payment card used;

(4) charging convenience fees for transactions for which the payment card is present, unless otherwise authorized; or

(5) providing discounts for payments made in cash.

[Adopted 2014-008 eff 1/14/2014]

38.095 Sanctions or Violations

(A) Failure to comply with this Policy and all other PCI-DSS carries severe consequences which may include the loss of the ability to process payment card transactions.

(B) Merchants will be held responsible for any losses, penalties, or punitive expenses incurred due to inadequate controls or failure to comply with PCI-DSS, including but not limited to any and all fees or fines associated with non-compliance or a security breach.

(C) Officials or employees who retain and misuse or share cardholder information may be subject to investigation, disciplinary action up to and including termination of employment, and potentially criminal prosecution.

[Adopted 2014-008 eff 1/14/2014]

38.100 Periodic Review

The PCI Compliance Manager shall review this Policy not less than annually and in response to significant operational changes or changes to the PCI-DSS and modify the Policy as necessary to continue to reasonably and appropriately protect cardholder information.

[Adopted 2014-008 eff 1/14/2014]

Statutory References and Other Authorities:
ORS 203

Legislative History of Policy No. 38:
Adopted 2014-008 eff 1/14/2014
Amendments to2014-008:
#1 none
