SECTION:	**Financial Management**	**POLICY #:**	**493**
TITLE:	**Merchant Cards**	**PROCEDURE #:**	**493-A**
		ORDER #:	**13-66**
DEPT:	**Treasurer's Office**	**DIVISION:**	**N/A**
ADOPTED:	**2/11** **REVIEWED:**	**REVISED:**	**6/13**

PURPOSE: This establishes policy for receiving and processing merchant card transactions and complying with security requirements set forth by the Payment Card Industry.

AUTHORITY: The Marion County Board of Commissioners may establish rules and regulations in reference to managing the interest and business of the county under ORS 203.010, 203.035, 203.111, and 203.230.

APPLICABILITY: Elected officials, department heads, managers, supervisors, and employees who process, transmit, handle, or store cardholder payment information in any physical or electronic format.

GENERAL POLICY: Ensure county employees protect cardholder information against theft and/or improper usage, comply with all credit and banking industry security regulations related to payment card processing and reporting, and maintain proper financial controls in the receipt and processing of payment card transactions.

POLICY GUIDELINES:

1. Definitions:
   - 1.1 Acquirer: a bankcard association member that initiates and maintains relationships with merchants that accept Visa, MasterCard, or Discover cards. Also referred to as "acquiring bank" or "acquiring financial institution".
   - 1.2 Breach: an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an unauthorized individual.
   - 1.3 Cardholder Information: any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, service code, and card validation code.
   - 1.4 Merchant: the Marion County department that accepts merchant cards for goods or services provided.
   - 1.5 Merchant Card: see Payment Card (also called Branded Card, Credit Card, Debit Card, and Payment Card). Those cards used to pay for goods or services with a logo on the face of the card (i.e., Visa, MasterCard, and Discover).

1.6 Merchant Card Processor: the vendor selected by the Treasurer's Office through competitive selection to process payment cards on behalf of Marion County.
1.7 Merchant Identification Number (MID): a unique number assigned to each terminal location or E-Commerce site that is used to track financial activity.
1.8 Payment Card: see Merchant Card (also called Branded Card, Credit Card, Debit Card, and Merchant Card). Those cards used to pay for goods or services with a logo on the face of the payment card (i.e., Visa, MasterCard, and Discover).
1.9 Payment Card Industry (PCI): a council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International on September 7, 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.
1.10 Payment Card Industry Data Security Standard (PCI-DSS) also called PCI Compliance: a series of requirements for handling, transmitting, and storing sensitive data.
1.11 PCI Compliance Manager: the County Treasurer or designee responsible for developing, implementing and updating the procedures required by this chapter, as well as other duties specified within.

2. Requirements:

The Payment Card Industry Data Security Standard sets forth twelve requirements for all merchants as follows:

2.1. Install and maintain a firewall configuration to protect cardholder data.
2.2. Manage passwords and other security parameters.
2.3. Protect stored cardholder data.
2.4. Develop encryption protocols.
2.5. Install and maintain anti-virus software or programs.
2.6. Develop and maintain secure systems and applications.
2.7. Restrict computer access to cardholder data.
2.8. Manage unique identification for each person with computer access to cardholder data.
2.9. Restrict physical access to cardholder data.
2.10. Track and monitor all access to network resources and cardholder data.
2.11. Test security systems and processes.
2.12. Maintain a policy that addresses information security.

3. Responsibilities:

3.1. The Treasurer's Office is responsible for overseeing all payment card transactions accepted for the sale of goods and services within the county departments.
3.2. The Treasurer's Office will partner with its sponsoring merchant card processor (Visa/MasterCard/American Express/Discover) and merchant card acquirer for all payment card transactions accepted for the sale of goods and services by all county departments.
3.3. The Treasurer's Office will ensure that any Merchant Card Processor doing business with Marion County will provide proof of compliance with PCI-DSS annually or when any change is made to software or hardware used for card transactions.
3.4. The County Treasurer or designee will be the PCI Compliance Manager for the county. The PCI Compliance Manager is responsible to develop, implement, and update the procedures required by Marion County and the Payment Card Industry, provide training and education

on payment card processing and security, notify appropriate parties of a suspected breach, and manage the county's PCI-DSS activities.

3.5. Departments interested in accepting merchant cards for goods or services must apply to the Marion County Treasurer's Office by submitting a Merchant Account Application.

3.6. Merchants are responsible for ensuring that all business processes for accepting, processing, retaining, and disposing of cardholder data comply with PCI-DSS and all other applicable policies and standards.

3.7. Merchants must ensure that all employees that may process, transmit, store, reconcile, or otherwise handle merchant cards attend merchant card training.

3.8. 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. A copy must be retained in the employee's departmental file.

3.9. Department employees that may process, transmit, store, reconcile, or otherwise handle merchant cards must comply with this policy; including, all relevant PCI-DSS requirements, Merchant Card Processing training attendance requirements, and signing the Merchant Card Compliance Statement.

3.10. Department employees must immediately notify the PCI Compliance Manager and their supervisor upon discovery of a breach or potential breach of cardholder personal information.

3.11. The Information Technology Department is responsible to approve and/or implement all computer networking, computer programming, and information system services necessary for the departments to provide merchant card services to the public in a manner that is compliant with PCI-DSS.

3.12. The Information Technology Department is responsible to work with the PCI Compliance Manager to meet PCI-DSS requirements related to information systems and provide documentation to the PCI Compliance Manager as necessary.

4. Security/Destruction of Cardholder Information:

4.1 Marion County will comply fully with all Payment Card Industry Data Security Standards to ensure the safekeeping and proper destruction of cardholder information.

4.2 In the event that cardholder personal information may be compromised, Marion County will take immediate steps to work with the merchant card acquirer and processor for appropriate action and notifications.

5. Fees:

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

6. Sanctions/Violations:

6.1. Merchants will be held responsible for any losses, penalties or punitive expenses due to inadequate controls or failure to comply with Payment Card Industry Standards. Merchants are responsible for any and all fees or fines associated with a non-compliance or security breach.

6.2. Employees who retain and misuse or share cardholder account data are subject to

investigation, disciplinary action, and/or termination of employment, and may also be subject to criminal prosecution.

6.3 Failure to comply with this policy and all other PCI-DSS requirements carries severe consequences which may include the loss of the ability to process merchant card transactions.

7. Periodic Review:

The PCI Compliance Manager shall review this policy not less than annually and in response to significant operational and legal changes, and modify the policy as needed to continue reasonable and appropriate protection of cardholder information.

Adopted: 2/11

Revised: 6/13