Table of Contents

1. Purpose

This policy sets forth requirements to be followed and provides guidance for the compliance with industry standards for payment card processing. The establishment of control measures for payment card transactions is necessary to maintain proper security over payment cardholder information.

2. Scope

Any employee or contractor with responsibilities for managing payment card transactions, and those who are entrusted with handling cardholder information must be familiar with, understand, and comply with this policy.

3. Requirements for Payment Card Processing

- Approval from the Board of Finance (NMAC 2.60.8) for the entity to accept payment cards and compliance with conditions in that regulation. Approval should be maintained by the entity. Modifications to or extensions of process should be discussed with BOF to determine if changes should be reviewed. Additional activities could impact and increase applicable section of PCI-DSS that agency must comply with.

- CIO or Payment Card Contact approval prior to entering into any contracts or purchases of software and/or equipment. This requirement applies regardless of the transaction method or technology used (e.g. point-of-sale device, payment gateways).

- Agency designs and selects cardholder acceptance process that triggers the least number of PCI-DSS requirements while still satisfying business needs.

- Employees and contractors processing payment cards are to attend card security training before beginning to process payment card transactions and at least annually thereafter.

- Comply with procedures for safeguarding cardholder information and secure storage of data. This pertains to ALL transactions initiated via the telephone, over the counter, Internet, etc.

- IT staff or Payment Card Contact will conduct periodic reviews of safeguarding and storage of cardholder information.

- Payment Card handling procedures are additionally subject to audit by internal audit, external audit or charge card review firms.

4. Policy

4.1. Management of cardholder information

Card Processors and Supervising Management – Ensures the following standards are maintained:

- Keep secure and confidential all cardholder data (CHD).
- Payment Card receipts should be handled as if they were cash.
- Create and maintain a ***Procedures for Handling Payment Card Data*** procedure to be reviewed and updated annually.
- Require all personnel involved in payment card handling to read and sign the ***Procedures for Handling Payment Card Data on an annual basis.***
- Ensure the entity does not store or retain payment card numbers after processing.
- Ensure payment card transactions are only conducted on secure computers or other authorized point of sale devices.
- Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data, ***CANNOT BE STORED*** in any fashion (paper, computers, etc.).
- Payment Card numbers must **NOT** be transmitted in an unsecure manner, such as by e-mail, unsecured fax, or through postal mail.
- E-mails received containing payment card numbers should not be accepted. The payment card number should be deleted and then a response may be sent to inform the individual that for their security, the Department does not accept payment card information through e-mail. The e-mail should then be deleted and emptied from the *Trash Folder*.
- If stored, payment card receipts to be retained for the period in the records retention guideline. If that is silent, then 18 months (or less) in a "secure" environment with access limited to dependable, trustworthy and accountable staff. Receipts must not contain the full payment card number, expiration date, or security code. Secure environments include locked drawers, file cabinets in locked offices, locked storage facilities, and safes.
- If payment card information is collected or submitted on an intake form, the payment card number must be cut off and destroyed by cross cut shredder immediately after transaction is complete.
- All payment card receipts must be destroyed in a manner that will render them unreadable at the records retention expiration mark. Records reaching their expiration date must be destroyed by a cross cut shredder, and their destruction documented OR the records may be securely destroyed by an

outside vendor (under the watch of the agency) in order to provide verifiable destruction dates.

4.1.1. Restrict access to payment card data and processing to appropriate and authorized personnel.

- Establish appropriate segregation of duties between payment card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all card refunds is required.
- Perform an annual self-assessment to ensure compliance with this policy and associated procedures.
- Notify CIO or Payment Card Contact prior to implementation of any changes affecting transaction processing associated with the payment card accounts.
- Background checks must be performed on all individuals (contractors, staff) involved in payment card handling prior to beginning work.
- Require all personnel involved in payment card handling to attend payment security training annually. Limit access to system components and cardholder data to only those individuals whose job requires such access.
- Maintain an updated list of authorized payment card processing personnel, authorized computers or other media (forms, hand held units, etc.).

4.2. IT or Payment Card Contact

- Review and approve implementation of any technology changes and payment gateways associated with payment card transactions processing.
- Conduct periodic reviews for compliance with Payment Card Industry (PCI) Data Security Standards (DSS).
- Collaborate with all divisions to complete the SAQ (security self-assessment questionnaire).

4.3. Information Security Incident Response Policy

Current department policies and procedures ensure timely and effective handling of any breaches in security related to cardholder data. It is important that this be reported immediately to the CIO or Payment Card Contact and the State's PCI-DSS Steering Team.

For a listing of current Steering Team Members please refer to the DFA Board of Finance Payment Card website.