INSERT DIVISION NAME/LOGO

Merchant Payment Systems Data Security

Policy and Procedure Template

**Department Name:**

**Division Name:**

**Business Process Owner/Title:**

**Last Reviewed:**

**Purpose**

The purpose of this policy is to establish business processes and **procedures for accepting and handling payment card, bank account and routing number information** at **INSERT DIVISION NAME** as established by the **Payment Card** Industry Data Security Standards (PCI DSS)[[1]](#footnote-1), National Automated Clearing House Association (NACHA)[[2]](#footnote-2) and in accordance with the policies promulgated by the Department of Technology and Information (DTI)**.** In order to maintain compliance with PCI DSS and NACHA, it is essential that agencies that store, process, or transmit cardholder data (CHD), bank account and routing number information adhere to procedures aligned with statewide and industry standards to help ensure the safe handling of payment data.

Collection and processing of automated clearing house (ACH), debit and credit card payments, will be conducted in compliance with standards established by the **Payment Card** Industry Security Standards Council (PCI SSC), NACHA, State of Delaware policies established by the Division of Technology and Information (DTI) and Office of the State Treasurer (OST), and the procedures outlined in this document. This policy is reviewed on an annual basis to ensure operational processes are documented and known to all affected parties and provided to agency personnel who are responsible for handling payment data.

**Business Process - Accepting and Handling Payments**

**User Access and Physical Security:** Access to **INSERT DIVISION NAME** payment system components and data is limited to only those individuals whose jobs require such access. Access to payment systems, including all in-scope applications and Point of Sale (POS) devices, are restricted based on job responsibilities. User access requests are submitted via helpdesk tickets to DTI and OST as applicable. Access to any payment system is role-based and permission is granted upon successful completion of PCI DSS training provided through the Delaware Learning Center (DLC). Upon hire, or upon the establishment of a new merchant account, the division’s business manager will notify OST of any new staff required to complete training.

When a user is terminated, transferred, or the job function no longer requires payment system(s)access, it is the Division’s responsibility to include the removal of system(s) access in their offboarding process, which includes notice to their Division IT representative

Devices that capture payment card data via direct physical interaction with the card should be physically secured and protected from tampering and substitution. This includes inspection once each one to three months of Point of Sale (POS) device surfaces to detect tampering. User access to sensitive areas that store, process, or transmit payment data is restricted based on job function.

**Annual PCI DSS Awareness Training:** In accordance with PCI DSS Requirement 12.6.1, all users within the **INSERT DIVISION NAME** authorized to handle payments will complete the PCI DSS awareness training found within the DLC annually. The annual PCI DSS training is intended to promote employee awareness of technical and operational requirements to protect all forms of payment data.

**Payment Card Terminals:** Purchase or rental of payment card terminals, including mobile applications, must be coordinated through OST – only devices and locations that have been approved and tracked by OST and DTI may be used in any way associated with payment processing. All devices must meet PCI DSS software and hardware standards[[3]](#footnote-3). The division is responsible to ensure that only authorized staff have access to the terminal(s) and are properly trained. Terminals must be inventoried with OST and must be maintained in a secure location. Sharing or transfer of wireless terminals between divisions is not allowed without proper approval from OST. It is the division’s responsibility to coordinate efforts with OST to ensure that terminals are updated with the most recent software version to reduce processing errors and to maintain data security.

Divisions may use rented wireless terminals on a temporary basis to accept in-person card payments at specified times as agreed upon in a rental agreement. If terminals are used on an intermittent basis they shall be kept in a secured location/locked when not in use. The procedures outlined in this document apply to both rented and purchased terminals.

**Batch Settlement:** Transactions must be settled no less frequently than daily. It may be prudent, given the level of activity, to settle batches on a more frequent basis. The division must maintain for a minimum of seven years all signed receipts and Batch Total Settlement Reports.

**INSERT NAME OF PAYMENT SYSTEM(S)** settles each night automatically. At 12:00 EST, a batch for each merchant is closed for the day’s activity and sent to the credit card processor. Funds are posted to First State Financials (FSF) based on the division’s merchant account ID – an account ID provided to OST and the division at the time an account is established. Divisions will establish and maintain appropriate segregation of duties between payment processing, processing of refunds, and the reconciliation of transactions. Each division is responsible to reconcile sales transactions to their general ledger no less than monthly.

**Disputes and Chargeback:**  The merchant processing provider or gateway product provider will receive and report chargebacks and transaction disputes to the division. Divisions can either accept or reject the chargeback. If rejected, the division will provide supporting documentation to justify that the transaction is valid. Failure to respond within the allocated timeframe will result in a loss of the transaction to the division. Prompt attention to these matters is a priority. It is the division’s responsibility to develop appropriate internal controls to mitigate risks related to chargebacks.

**Physical Security Procedures**:

1. Upon hire, staff are trained to follow standards established by the PCI SSC, NACHA, DTI, OST, **INSERT DIVISION NAME**, and the operational procedures outlined in this document. In addition, staff are trained to be aware of methods in which devices can be tampered with or replaced. Training includes the following practices are adhered to:
	1. Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices;
	2. Being aware of suspicious behavior. For example, attempts by unknown persons to unplug or tamper with devices, computers with payment applications, and websites that host payment applications; and
	3. Not altering or directly attempting to troubleshoot terminals. Troubleshooting support is provided by OST and/or DTI.
2. At the start of each day (prior to use), the terminal surfaces are checked to detect tampering or substitution. At a minimum of each one to three months, an in-depth assessment of all terminals is conducted using the Merchant Tampering Checklist **(INSERT FILE LOCATION)**, verifying that the device(s) has not been swapped with a fraudulent device by performing the following steps:
	1. Compare the serial number and model number listed on the terminal to that included on the PCI Asset Inventory Tracking Sheet;
	2. Review the tamper evident stickers on the surface of the terminal and make sure it is intact;
	3. Inspect the terminal and review for foreign objects (i.e. skimmers), unexpected attachments or cables plugged into the device, pry marks, broken or stressed seams;
	4. If you notice anything unusual or suspect that the terminal has been tampered with or substituted, contact OST and DTI immediately at pci\_compliance@delaware.gov and DTI\_ServiceDesk@delaware.gov; and
	5. When mobile terminals are changing hands between users, an additional tamper check will be performed by the section manager responsible for payments at the end of that business day.

**Payment Processing Procedures:**

1. **Mail Order – The division receives mail orders for INSERT BUSINESS REASON(S) and payment information is returned on a form.**
	1. Mail is sorted and opened by two staff members; payment forms with sensitive data are separated from checks.
	2. Forms with payment data (credit, debit, bank account, or routing information) are placed in a pouch and kept locked in a Manager’s office until a processor is available to process the transaction, which shall occur either the same or next day.
	3. Staff enter the payment information into an encrypted web based or point of sale terminal:
		1. If approved, the payment data on the original form is shredded. If an agency has a business need to retain information on an order form, the payment information section must be separate from the other information on the form so that it can be detached and appropriately destroyed upon payment processing; or
		2. If declined, that transaction and all the backup associated with the transaction is removed from the batch and stored in a secured location while the issue is resolved. Once resolved, the previous instructions for an approved transaction apply.
	4. Any uncharged transactions remaining at the end of the day are stored in a secured location.
2. **Fax Order – The division receives orders via secure fax at INSERT FAX NUMBER**
	1. Faxes with payment information are immediately removed from the fax machine and distributed to the appropriate personnel who is to perform the transaction.
	2. If faxes are received via a fax device, including multifunction copier, the division must ensure that the device is not storing document information electronically.
	3. Steps 1c and 1d are followed.
3. **Phone Order – The division will accept payments via phone only to INSERT DEDICATED PHONE NUMBER**
4. Payment information should be taken and entered directly into point of sale and virtual terminals. No numbers or other payment information will be written down.
5. If payment information is written down by hand, the same procedure outlined under Mail Order shall be followed as outlined above. No payment information shall be recorded or stored electronically after authorization.
6. Confirmation Number will be given to customer once the transaction is processed.
7. **Email Orders are Not Permitted – the division does not accept payments sent in via email.**
8. The payment will NOT be processed.
9. If payment data is received via email, a response will be sent to the customer. The response will be a separate email – not a response to the original email, indicating the policy and procedure for sending payment information.
10. The original email will be permanently deleted from email inbox and trash folder.
11. **In Person – The division accepts payments in person at INSERT ADDRESS(ES).**
12. Request card from cardholder for processing. Ensure card is signed, if not, request ID.
13. Process transaction via point of sale terminal, kiosk or virtual terminal.
14. Have customer sign merchant copy/receipt. Verify signature matches back of card.
15. Give card and receipt to customer.
16. **Online Orders**
	1. Online orders are taken via the division’s online solution at **INSERT URL**(s).
	2. Only individuals with authorized access to the online systemwill fulfill orders on a daily basis.

**Refund Procedures:**  Clear disclosure of return, refund, and cancellation policies can help to prevent potential customer disputes and chargebacks. Card brands will support refund policies provided they are clearly disclosed to cardholders. Divisions using various payment systemsmust communicate refund/return/cancellation policies to their customers including offering disclosures on their website or available in person.

1. The Division’s refund policy can be located at INSERT LINK
2. Procedures to refund a credit card transaction are included in the user manual for the POS devices and **INSERT NAME OF SYSTEM(S) (if applicable)**.

**Incident Response Procedures:** An incident is defined as a suspected or confirmed data compromise in which there is a potential impact to the confidentiality or integrity of payment data.  A data compromise is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted payment data is collected, processed, stored, or transmitted. In the event of a suspected or confirmed incident:

1. Call the DTI Help Desk at 302-739-9560 and contact OST at**pci\_compliance@delaware.gov**.
2. Do not turn off the compromised point of sale machine(s) or computer(s) processing payments. Unplug any and all network (internet) cables connected to point of sale machines.
3. Do not attempt to use or troubleshoot any of the compromised systems.
4. Wait for further instructions from DTI before taking additional steps.
1. <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security> [↑](#footnote-ref-1)
2. <https://www.nacha.org/rules/supplementing-data-security-requirements> [↑](#footnote-ref-2)
3. <https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement?return=%2Fassessors_and_solutions%2Fpayment_applications> [↑](#footnote-ref-3)