Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

BACKGROUND

State of Wisconsin agencies accepted more than 6 million credit/debit card payments annually through the following payment methods:

- Point of Sale (State agency location)
- Point of Sale (Retail-agent location)
- Mail Order
- Telephone Order
- Fax
- Paper Lockbox
- Internet (Electronic Lockbox)
- Internet 3rd Party (When the State of Wisconsin does not own the MID)

The purpose of this document is to establish internal control procedures for agencies to follow when accepting credit/debit card payments through these channels. These procedures are necessary to protect agencies and their customers from financial loss due to fraud or human error. In addition, the procedures mirror the Payment Card Industry (PCI) standards related to the acceptance of credit/debit card payments. In addition, Section 19.36(13) Wisconsin Statutes, prohibits access to cardholder information:

13) Financial identifying information. An authority shall not provide access to personally identifiable data that contains an individual's account or customer number with a financial institution, as defined in s. 895.505 (1) (b) including credit card numbers, debit card numbers, checking account numbers, or draft account numbers, unless specifically required by law.

Failure to follow the following procedures may subject the state to significant losses, including:

- Fines from Visa, MasterCard, American Express and Discover;
- Payments to cardholders for actual fraud losses that result from the theft of their card information;
- Cost of providing credit monitoring to affected cardholders;
- The cost of reissuing cards to those cardholders who had their information compromised (approximately $2 to $10 per card);
- Media coverage resulting in decreased confidence in the use of electronic payment methods by state customers.

Because of the significant loss that can result from the theft of cardholder information, state agencies are expected to comply with these internal control procedures. The procedures will be audited by the State Controller's Office – Internal Audit Section.

Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

POLICIES

1. State agencies may only use the enterprise contracts for E-Payment Gateway Services (aka the payment pages), and Merchant Processing and Acquiring Services (aka the credit/debit card processing). For a depiction of the State's credit/debit card processing, please see the website: http://doa.wisconsin.gov/Documents/DEBF/SCO/Treasury%20Services/Treasury%20Documents/creditdebit%20flowchart.pdf Please note that these enterprise services do not include building the web store front. If any agency utilizes a vendor for storefront services, they must ensure that the vendor is compatible with the enterprise contracts for E-Payment Gateway and Merchant Processing Services.

PROCEDURES

INTERNAL CONTROL PROCEDURES BY PAYMENT CHANNEL

Point of Sale (POS) Terminals (i.e. transactions swiped or keyed into a POS terminal)
Credit/debit card operating rules prohibit merchants from printing the full 16 digit card number on the customer copy of the receipt issued through a point of sale terminal. In addition, Section 134.74(2), Wisconsin Statutes states:

Beginning on August 1, 2005, no person who is in the business of selling goods at retail or selling services and who accepts a credit card or a debit card for the purchase of goods or services may issue a credit card or debit card receipt, for that purchase, on which is printed more than 4 digits of the credit card or debit card number.

Internal Control Procedures

1. State agencies should never print the full 16 digit card number on either the merchant or customer copy of the point of sale receipt. A merchant copy of the receipt containing the authorization number and only 4 digits of the card number is sufficient for responding to all cardholder disputes/charge backs.

2. POS Terminals must be implemented using a dial-up connection, unless:

   a. There is a unique business need; and
   b. The application is approved by the State Controller's Office; and
   c. The application has achieved PCI Certification before going live.

3. The merchant copy of the POS receipt should be attached to a copy of the agency sales receipt that was provided to the customer.

Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

4. Per credit card operating rules, the merchant copy of the point of sale receipt should be retained for a period of 3 years.

5. Point of Sale devices used by State agencies should never store magnetic stripe (track) data, CID, PINs, or encrypted PIN blocks.

6. All Point of Sale terminals are required to be password protected and/or locked in a secure location when not in use.

7. Access to POS Devices and payment applications should be controlled and limited to employees who require access to these POS devices or payment applications to complete their jobs. This access is restricted specifically for only what employees require to do their job.

Mail Order, Telephone Order or Fax Order

Agencies may receive cardholder information via mail order, telephone order or fax order. These payment channels are discouraged because of their high labor cost, and the higher interchange rates associated with keying the information into a Point of Sale Terminal.

In addition to the internal control procedures listed above for transactions swiped or keyed into a POS terminal, the following internal control procedures should be followed for these paper-based transactions.

Internal Control Procedures

1. Agencies should process mail order, telephone order or fax orders through a POS terminal. **Agencies must never key cardholder information into a workstation that is on a state computer network**.

2. State agencies should obtain the cardholder information on a separate form (i.e. the card holder information should not be part of the agency's primary remittance document).

3. Once the credit/debit card payment has been authorized, the merchant copy of the point of sale receipt (including the authorization number) should be attached to the agency remittance document.

4. Once the credit/debit card payment has been authorized and the authorization number recorded, the agency form that contains the card holder information should be securely destroyed.

Lockbox

Some paper lockbox applications allow for payment via check or credit card.

Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

Internal Control Procedures

1. State agencies should obtain the cardholder information on a separate form (i.e. the cardholder information should not be part of the agency's primary remittance document).

2. The bank lockbox staff will enter the cardholder information into their credit/debit card processing system and receive either an authorization (approval) code or a denial. Bank staff will write either the approval (authorization) code or the word "denied" on the remittance document. The bank will retain the cardholder information for not more than 30 days at which time the form will be securely destroyed.

3. The authorization number on the remittance document will allow the agency to reference the transaction through the merchant processor's online transaction system.

Electronic payment channels

The State's Enterprise E-Payment Process utilizes "hosted" credit/debit card payment pages for accepting payments online. The hosted solution also allows for the registration of credit/debit cards and bank accounts for recurring payments. The solution complies with Visa, MasterCard, American Express, and Discover credit/debit card operating rules, and with the National Automated Clearing House (NACHA) operating rules.

This hosted E-Payment gateway results in the indemnification of state agencies from any potential liabilities resulting from compromised cardholder information, because the information only exists at the state's E-Payment gateway provider.

Internal Control Procedures

1. State agencies should never collect, enter or store cardholder information on a state computer system. Cardholder information should be collected on a payment page that is hosted by the E-Payment gateway provider.

2. Agencies should never store cardholder information in an electronic format. This includes but is not limited to computer programs, databases, spreadsheets or word processing documents.

3. The E-Payment gateway provider will retain the cardholder information necessary to comply with the card company operating rules.

Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

Additional procedures

Agencies should utilize the following additional internal control procedures:

1. Cardholder information should never be emailed.

2. State agency staff should always authenticate a Payer before discussing cardholder information over the telephone. This can be done with a telephone number, email address or a shared secret.

3. Refunds of credit/debit card payments should be made by staff that does not have responsibility for reconciliation.

4. Each agency should require explicit approval to use POS Terminals or to complete mail, telephone or fax order technologies. Management is required to maintain a list of authorized personnel and devices.

5. Each Agency should review their policies at least once per year or any time a change is made that would alter an existing policy or procedure for securing relevant paper and card processing devices.

6. The State Controller's Office must approve:

    - New merchant accounts/id's;
    - Changes in merchant processing providers for existing merchant accounts;
    - New E-Payment applications.

7. Convenience fee charges must comply with State Statutes and policies issued by the Depository Selection Board (DSB) per Section 20.905(1), Wisconsin Statutes. See Wisconsin Accounting Manual Section 06-05 for the current policies.

8. State agencies shall not allow credit/debit card processors to debit State bank accounts for their monthly fees, or to net credit/debit fees against settlement deposits.

9. Credit/debit card processing fees shall be accounted for according to Section 06-05 of the Wisconsin Accounting Manual.

10. On a daily basis, accepted credit/debit card transactions shall be reconciled to bank deposits, and recorded into the State's accounting system.

11. Merchant billing statements shall be compared monthly to contact pricing.

Section	14	INTERNAL CONTROLS	Effective Date	7/1/2015
Sub-section	04	Internal Control Procedures for Accepting Credit/Debit Card Payments	Revision Date	12/12/2109
SAM Ref	n/a			

Complying with the Payment Card Industry (PCI) Standards

Any agency who maintains a Merchant Account for accepting credit/debit card payments must be in compliance with the PCI security standards. The State Controller's Office will coordinate PCI compliance with each agency. The key element in the compliance process is the internal control procedures established within this document.

Reporting a Security Incident

Even though the necessary precautions are in place for cardholder data security any incidents of theft or fraud of cardholder data must be reported immediately to the PCI Coordinator in the State Controller's Office. The PCI Coordinator will establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

Incident Identification: Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their daily activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within the databases, logs, files, or paper records.

Reporting an Incident: The PCI Coordinator must be notified immediately of any suspected or actual incidents involving cardholder data. Document any information you know related to the incident such as date, time, and nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response: The PCI Coordinator will notify the necessary parties involved as needed. The PCI Coordinator will also work with the agency to eliminate potential risks going forward.