# State of Maine
# Office of the State Treasurer
## Credit Card Information Security
## Policy & Guidelines

## Purpose

To ensure the safety of State of Maine customer's financial data by establishing guidelines for processing charges/credits on Credit Cards to protect against the exposure and possible theft of account and personal cardholder information that has been provided to the State of Maine and to comply with credit card industry requirements for transferring credit card information.

This policy may not be inclusive of all risks. Department management should use sound judgment in assessing additional risk and implementing more strict guidelines that best fit their department.

## Scope

This policy applies to all State of Maine employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any department/bureau/unit/division that processes, transmits, or handles cardholder information in a physical or electronic format.

## Policy

1. The Office of the State Treasurer must approve all credit card processing activities in the State of Maine prior to entering into any contracts or purchasing equipment. This requirement applies regardless of the transaction method (e.g. online processing, outsourced to a third party, or swipe terminals).

2. Departments approved for credit card processing activities must maintain the following standards:

A. Cardholder Data

- The Primary Account Number (PAN) should **NOT** be stored on any system, personal computer or email account. (Should your department have a legal or regulatory requirement to store the PAN, permission may be granted only after a written request has been reviewed and approved by the Office of the State Treasurer. Additional restrictions will apply)

- Under no circumstances should the card verification code or value or PIN number or value be stored.

- Do not store the full contents of any track from the magnetic stripe.

- Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)

- Keep all other cardholder data storage to a minimum. Develop and document a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and or regulatory purposes, as documented in retention policy. Cross cut shred, incinerate, purge, degauss, or shred any hardcopy or electronic media when it no longer qualifies for storage under the retention policy.

B. System Requirements

- Install and maintain a firewall configuration capable of protecting cardholder data

- Encrypt transmission of cardholder data across open, public networks, including wireless networks.

- Use and regularly update anti-virus software or programs. Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

- Develop and maintain secure systems and applications. All systems must have the most recently released, appropriate vendor provided security patches. Establish a process to identify newly discovered security vulnerabilities.

- Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.

C. Access Control

- Limit access to computing resources and cardholder information only to those individuals whose job requires such access.

- Identify all users with a unique user name before allowing them to access system components or cardholder data. Authentication must be used in the form on one or more of the following methods: Password, Token Devices (SecureID, Public Key), Biometrics.

- Ensure proper user authentication and password management. This includes: Modifications of user IDs, addition, deletion, removal of inactive accounts, immediate revocation of terminated users, password lockout, inactivity logout, authentication of all access to any database containing cardholder data.

- Physically secure all paper and electronic media (including computers, networking and communications hardware, paper receipts, reports, and faxes) that contain cardholder data.

- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process or transmit cardholder data.

D. Security Policy

- Develop and maintain department specific credit card security procedures.

- Develop usage policies for employees and contractors containing acceptable uses of technologies.

- Implement formal security awareness training to make all employees aware of the importance of cardholder data security.
- Require employees to acknowledge in writing that they have read and understood the department's security policy and procedures.

- Create an incident response plan to be implemented in the event of a system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies.

E. Payment Card Industry Data Security Standard

- The PCI DSS establishes industry standards concerning the handling of credit card data. In addition to compliance with the Treasurer's Policy, departments should be thoroughly familiar and in compliance with the PCI DSS where applicable. The Treasurer's office will provide your Department with the PCI DSS upon setup and before approval.

- Departments may consider contracting with a vendor to scan each IP connection and/or website to ensure PCI compliance.

- Departments using only a dial terminal may contact the Treasurer's Office for a self-assessment questionnaire.

## Procedure

The Office of the State Treasurer must approve all credit card processing activities in the State of Maine prior to entering into any contracts or purchasing equipment. This requirement applies regardless of the transaction method.

Departments who need to process credit/debit cards should contact the Director of Internal Operations to begin setup. The Director will facilitate the setup of services with the banking institution and establish the necessary merchant number(s).

Departments are responsible for the related setup and merchant fees associated with their accounts. Once setup is underway, the department head or delegate must complete the Office of the State Treasurer Credit Card Information Security Policy Acknowledgement and Agreement form acknowledging receipt and compliance of the security policy and the associated PCI DSS. This certification will also include a statement that the department has confirmed that sufficient allotment exists and is budgeted for the merchant fees associated with the new/existing merchant account.

## Penalties

Failure to comply with the PCI DSS can carry fines of $500,000.00 per offense, and can include revocation of credit card processing capabilities. Department management should understand the risks involved and take all actions necessary to ensure credit card security.

# Resources

***To be used in conjunction with the State Treasurer's Credit Card Information Security Policy & Guidelines***

The PCI DSS (Payment Card Industry Data Security Standards) specification can be found at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

The PDI DSS Self-Assessment Questionnaire can be found at: https://www.pcisecuritystandards.org/saq/index.shtml.

For the application form to create a new merchant account, please contact Kristi Carlow at Kristi.L.Carlow@maine.gov.