



**Arizona State Treasurer's Office
Request for a Merchant ID (MID) and
Payment Card Industry Data Security Standard (PCI-DSS) & Merchant Responsibilities
Acknowledgement**

To support an agency's decision to become a "merchant," allowing it to accept and process credit cards, the State Treasurer's Office administers the State of Arizona's Merchant contract and registration.

State agency merchants are subject to, must understand, and comply with all rules, regulations and contractual provisions regarding the handling of payment cards. The regulations include the Payment Card Industry Standards and the Card Association's (representing MasterCard, VISA, American Express and Discover Card) merchant requirements. All state agency "merchants" are required to comply with these regulations and requirements to continue to accept payment cards. In the event of non-compliance, the State Treasurer's Office reserves the right to revoke those privileges until such time as compliance is achieved.

To assist agencies, the State Treasurer's Office and ADOA-ASET have contracted with online service providers to offer State agency merchants with Payment Card Industry Data Security Standard (PCI DSS) compliant options for accepting online credit card payments.

Non-compliance with the Payment Card Industry standards puts the State of Arizona at risk for:

- Large monetary fines assessed to your agency and/or the State Arizona
- Loss of merchant status for your agency
- Possible loss of merchant status for all of State of Arizona Government

General Rules, Regulations, and Guidelines

A) Security

1. All State of Arizona Agency "Merchants" are required to review the Payment Card Industry Data Security Standard (PCI DSS) located online at <https://www.pcisecuritystandards.org/>.
2. If your agency processes credit card data in any form (face-to-face or online), it needs to be in compliance with Payment Card Industry Data Security Standards (PCI DSS).

3. All eCommerce gateways need to be PCI DSS certified and compliant with the State of Arizona's security requirements.
4. All electronically captured information must be in an encrypted secure socket layer (SSL) that meets the PCI DSS requirements with minimum need-to-know basis access to cardholder information.
5. Any vendor technical documents provided to the Agency "Merchant" must be kept in a secure location and not shared with anyone without a valid need to know.
6. To meet the Arizona Revised Statute (A.R.S) § 18-545 (Notification of Breach of Security System), the PCI-DSS payment card industry provisions and requirements, all suspected and/or confirmed security compromises need to be reported immediately to the State Treasurer's Office and ADOA-ASET. If a breach has occurred with respect to the data stored by your agency, the agency will be responsible for any and all externally imposed fines as well as the costs associated with bringing your location into compliance.
7. It is prohibited to store card information and card-validation codes (three-digit value printed on the signature panel of a card) on any State of Arizona computer, database or server. Your agency must protect cardholder data by keeping it secure and confidential.
8. Your agency must not collect card numbers and card information via any non-secure medium such, but not limited to, e-mail, unsecured or network fax machines, or cell phones.
9. On behalf of your agency, you agree to maintain all card documentation containing card account numbers in a "secure" environment, restricting user access to payment card account numbers to a need-to-know basis. Secure environments include locked drawers, file cabinets in a locked office, and safes. Credit card receipts and card documentation need to be treated in the same manner you would treat large sums of cash. Your agency is responsible for any losses due to inadequate internal controls. All card account numbers must be cross shredded within twenty-four (24) hours of receipt and must comply with A.R.S. § 44-7601.
10. You agree that your agency will not disclose or acquire any information concerning a cardholder's account without the cardholder's consent. You or your agency will not sell, purchase, provide, disclose or exchange card account information or any other transaction information.
11. Your agency will treat the following as high-risk transactions: use of an anonymous e-mail address, shipping address from overseas, prisons, hospitals, or mail drops.

Name of State Agency: _____

Approval: _____
Agency Head Printed Name

Approval*: _____
Agency Head Signature Date

* By signing this form your agency is approving the establishment of this merchant account and assumes responsibility for compliance with the Payment Card Industry Data Security Standards and the State of Arizona policy and guidelines as outlined above and in the attached document.

- Please call 602-542-7844 or email PCI@aztreasury.gov.
- Please complete and return scanned copy to: banking@aztreasury.gov
State Treasurer's Office-Banking Division/PCI
1700 W. Washington STE 102
Phoenix, AZ 85007

Additional information on PCI DSS may be obtained by visiting the PCI Security Standards Council website at: <https://www.pcisecuritystandards.org>.