The Arizona State Treasurer's Office
PCI Information

Do's

- Must use the Arizona State Treasurer Office (ASTO) servicing and merchant bank contract for payment card acceptance.
- Process all card transactions using an ASTO approved method(s).
- Protect cardholder data as if it were cash.
- Restrict access to cardholder data to a need-to-know basis.
- All terminal and merchant accounts must be settled on a daily basis.
- Report any suspected theft or security breach immediately.
- If you have a form that contains pertinent information in addition to payment card numbers, consider having the payment card number on the bottom of the form so that this portion can be removed from the form once the payment has been processed and shredded the same day while maintaining the non-payment portion of the form.
- Please refer to Arizona Strategic Enterprise Technology Office (ASET) Statewide Policy at https://aset.az.gov/resources/policies-standards-and-procedures
- Please refer to General Accounting Office (GAO) for Statewide Policy https://gao.az.gov/publications/saam Section 40 topic 16.
- Contact the ASTO with any questions at PCI@aztreasury.gov

Don'ts

- Don't store payment card numbers on state systems including PCs, laptops, flash drives, servers, mobile devices, etc., in any format, including databases, spreadsheets, PDFs and scanned documents.
- Don't store magnetic strip cardholder data or the CVV or CVC code (the additional security number on the back of credit cards) after authorization.
- Don't use vendor-supplied, default system passwords or common/weak passwords.
- Don't store cardholder data in any systems in clear text (i.e., unencrypted).
- Don't leave remote access applications in an "always on" mode.
- Don't store physical copies of cardholder data past authorization unless a legitimate documented business need exists to maintain the information. Storing card information for a possible future refund is not a legitimate business purpose. If a refund needs to be completed at a later time, please contact the customer over the phone to collect the necessary information or use STATE web portals online refund feature. Contact OST or ASET for details.
- Don't create an online form or webpage that collects payment cards. Please contact either the ASTO or ASET.
- Don't dispose of reports, documents or receipts that contain cardholder data in the trash or recycle bin. The materials must be destroyed via a cross-cut shredder.
- Don't process any payment card information received via Email/Text/Chat (End User Messaging). Payment card numbers and authentication data must never be sent or received via email, text or chat. As a merchant you should discourage the sending of credit card information to the point of not processing credit card transactions when the information has been provided unsolicited over email. Respond back to your customers (first deleting or truncating credit card numbers and

deleting any authorization codes) and inform them of acceptable payment methods. Consider adding the following verbiage:

"For your protection, the State of Arizona does not accept, and will not process credit card information provided via email or text messages. Please contact us at (Agency fills in) or email us at (Agency fills in), and we will gladly assist you."

Additional Information (channel specific)

Fax

- Payment card numbers must not be received via fax machine unless the fax is a standalone fax machine connected to an analog telephone line (VoIP lines are not secure when receiving payment card information).

In Person

- Swipe the card if a swipe terminal is available.
- Do not process a card transaction where the name on the card does not match the Valid ID of the individual presenting it.

Voice Telephone Line (analog or VoIP)

- Ensure that voice phone calls are not recorded.

The ASTO PCI compliance team is available to address questions and work with you to ensure the very rigorous PCI compliance requirements are met. For more information visit the PCI Security Standards Council or contact the ASTO at PCI@aztreasury.gov .