State of Arizona Accounting Manual

INTRODUCTION

Payment card transactions and the systems that process them are constantly under attack by those attempting to acquire payment card information that may be used for illicit purposes. This information includes personal data such as Social Security Numbers, dates of birth, addresses, bank account numbers, medical data, etc.

To combat these attacks, the major credit card issuers created the Payment Card Industry Security Standards Council (hereinafter referred to as PCI).

The PCI requires all entities that store, process or transmit cardholder data to maintain appropriate safeguards over such data. Cardholder data includes any personally identifiable data associated with a cardholder such as account number, expiration date, card validation code, etc. This requirement extends to third-party vendors with whom the State or its agencies may contract to provide payment card processing services.

Failure to comply with the PCI standards—by the State, its agencies or those with which the State contracts to provide payment card processing services—may result in dire consequences, including substantial fines as well as the suspension or termination of the State's or an agency's merchant status (i.e., authorization and ability to use payment cards to expedite collections).

In the context of this section of SAAM, a payment card refers to either a credit card or a debit card used by an individual or organization to remit a payment to the State or to one of its agencies. It does not refer to the P-Card, CTA, ETC or other procurement or payment cards used by the State, its agencies or its personnel to effect a purchase or payment.

Payment card processing, as discussed herein, refers to the use of any application, device or manual procedure to accept remittances to the State for services, goods, taxes, fines, etc.

This is one of a series of SAAM sections dealing with PCI compliance.

POLICY & PROCEDURES

1. All third-party vendors directly involved in the collection, transmission or processing of cardholder data are required to provide annually, or more frequently upon a written request by the Office of the State Treasurer, a copy of a Payment Card Industry Data Security Standard (PCI DSS) Attestation of Compliance (AOC), validated by a Qualified Security Assessor (QSA).

2. All third-party vendors that can affect the security of the flow of payment card data, but are not directly involved in the collection, transmission, or processing of cardholder data, are required to provide annually, or more frequently upon a written request by the Office of the State Treasurer, a copy of the Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaire (SAQ) completed by the vendor.

2.1. An example of a vendor able to affect the security of the flow of payment card data, but that is not directly involved in the collection, transmission, or processing of cardholder data, would be a web-hosting provider that redirects users to a payment gateway, but who does not collect or retain credit card data on its website.

3. For the purposes of this policy, the following are <u>not</u> considered to be third-party vendors and are <u>not</u> required to provide either an AOC or an SAQ:

3.1. Any agency, division or unit of the Government of the State of Arizona.

3.2. The state-contracted servicing bank, when providing centralized payment card processing services.

4. Questions concerning compliance with this policy statement should be directed to the Office of the State Treasurer.