State of Arizona
Payment Card Incident Response Plan

To address payment card holder security, the major credit card brands (Visa, MasterCard, Discover, American Express and the Japanese Credit Bureau (JCB)) jointly established the Payment Card Industry (PCI) Security Standards Council to administer the PCI Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create an Incident Response Team and document an Incident Response Plan. The State of Arizona Payment Card Incident Response Team (Response Team) is comprised of the State Treasurer's Office, ADOA-ASET, ADOA-GAO and the Merchant Service Provider for the State of Arizona.

The Chief Information Security Officer (CISO) and the State Treasurer's Office lead the Response Team when an incident occurs. The team also includes representatives who will be notified as needed. The response team will determine who should be notified of the breach.

- Governor's Office
- Media Relations
- GAO Internal Audit
- Auditor General
- Office of Attorney General

(Suggestion, if your agency executive staff would like to be informed prior to reporting to the PCIResponse team, please add a line here indicating such)

1. All incidents must be immediately reported by contacting PCIResponse@aztreasury.gov.

2. The incident emails will notify all members of the Response Team.

3. The Response Team, along with the staff of the compromised agency, will investigate the incident and assist in limiting the exposure of cardholder data.

4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, payment card processors, etc.) as necessary.

5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Incident Response Plan

An “incident” is defined as a *suspected* or *confirmed* “data compromise.” A “data compromise” is any situation in which there has been **unauthorized access** to a system or network where cardholder data is collected, processed, stored or transmitted. A “data compromise” can also involve the suspected or confirmed loss or theft of any material, equipment or records that contain cardholder data.

In the event of a *suspected or confirmed* incident:

1. All incidents must be immediately reported upon discovery to members of the Response Team. Contact the Response Team by emailing PCIResponse@aztreasury.gov.

2. Immediately contain and limit the exposure and preserve evidence by taking the following steps:

    a. Do not access or alter compromised systems (i.e., don’t log on to the machine and change passwords, do not log in as ROOT).
    b. Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug Ethernet cable, disable wireless, etc.).
    c. Preserve logs and electronic evidence.
    d. Log all actions taken.
    e. Except for any systems believed to be compromised, change the Service Set Identifier (SSID) on any access point or any other devices that may be using this connection.
    f. Be on “high alert” and monitor all systems with cardholder data.

3. Document any steps taken until the Response Team has arrived. Include the date, time, person/persons involved, and action taken for each step.

4. Assist the Response Team as they investigate the incident.

5. If an incident of *unauthorized access* is **confirmed** and card holder data was potentially compromised, the Payment Card Coordinator with the State Treasurer’s Office will contact the Merchant Servicing provider and the System’s acquiring bank as follows:

For incidents involving **Visa, MasterCard or Discover network cards**, contact:

- Bank of America Merchant Services (Ernan Patawaran at 1-970-631-8265 (direct), 1-970-617-3650 (mobile), Ernan.Patawaran@BankofAmericaMerchant.com or

- Bank of America Merchant Services Customer Support (at 1-800-430-7161 or 1-800-228-5882 within 72 hours of the reported incident).

For incidents involving **American Express**, contact Enterprise Incident Response Program (EIRP):

- *EIRP (eirp@aexp.com, at 1-888-732-3750 or 1-602-537-3021).*

IT Security Incident Response Procedures

The Response Team will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. Work with relevant internal and external authorities.

(suggestion: add your agency's service providers information here for easy reference)