State of Alaska
Department of Revenue

Credit Card Policy for the State of Alaska

Prepared by:
SoA Security Office

Table of Contents

1 INTRODUCTION AND SCOPE

1.1 Introduction

The State of Alaska is required by the contract with our merchant card processor to achieve and maintain PCI compliance. This document explains State of Alaska's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. State of Alaska management is committed to these security policies to protect information utilized by State of Alaska in attaining its business goals. All employees are required to adhere to the policies described within this document.

1.2 Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, State of Alaska's cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, ver. 3.0, released February, 2014. Should State of Alaska implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of State of Alaska to determine the appropriate compliance criteria and implement additional policies and controls as needed.

http://treasury.dor.alaska.gov/CashManagement/CreditCardPaymentInformation.aspx

1.3 PCI DSS v3.1

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

PCI DSS Applicability Information *(PCI DSS page 7)*
PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. Cardholder data and sensitive authentication data are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
▪ Primary Account Number (PAN) ▪ Cardholder Name ▪ Expiration Date ▪ Service Code	▪ Full track data (magnetic-stripe data or equivalent on a chip) ▪ CAV2/CVC2/CVV2/CID ▪ PINs/PIN blocks

The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with applicable PCI DSS requirements.

PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE1. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

The table on the following page illustrates commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be protected. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

Scope of PCI DSS Requirements *(PCI DSS page 10)*

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. **The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.** Examples of system components include but are not limited to the following:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. To confirm the accuracy of the defined CDE, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined CDE.
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).

- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data.

The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.

2 SoA PCI Compliance policies

2.1 Requirement 1: Build and Maintain a Secure Network

Not required for Dialup solutions.

2.1.1 Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider (PCI Requirement 1.2).

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied (PCI Requirement 1.2.1).

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment (PCI Requirement 1.2.3).

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment (PCI Requirement 1.3.3).
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall (PCI Requirement 1.3.5).
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering (PCI Requirement 1.3.6).

Any mobile and/or employee-owned computers with direct connectivity the Internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users (PCI Requirement 1.4).

2.2 Requirement 2: System Passwords and Other Security Parameters

Not required for Dialup solutions.

2.2.1 Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts (PCI Requirement 2.1).

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to (PCI Requirement 2.1.1):

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

2.2.2 Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. State of Alaska must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards (PCI Requirement 2.2).

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (PCI Requirement 2.2.1).
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system (PCI Requirement 2.2.2).
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure (PCI Requirement 2.2.3).
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers (PCI Requirement 2.2.5).

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to insure that security parameter settings set appropriately on all system components before they enter production (PCI Requirement 2.2.4).

System administrators are responsible to insure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties (PCI Requirement 2.5).

2.2.3 Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following (PCI Requirement 2.3):

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

2.3 Requirement 3: Protect Stored Cardholder Data

2.3.1 Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable (PCI Requirement 3.2).
Payment systems must not store sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance (PCI Requirement 3.2.1).
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance (PCI Requirement 3.2.2).
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance (PCI Requirement 3.2.3).

2.3.2 Displaying PAN

State of Alaska will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following (PCI requirement 3.3):

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

2.4 Requirement 4: Encrypt Cardholder Data Across Open, Public Networks

2.4.1 Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, State of Alaska will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.). These controls will be implemented as follows (PCI Requirement 4.1):

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission (PCI Requirement 4.1.1).

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat (PCI requirement 4.2).

2.5 Requirement 5: Use and Update Anti-Virus Software or Programs

Not required for Dialup solutions.

2.5.1 Anti-Virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software (PCI Requirement 5.1, 5.1.1).

For systems considered to be not commonly affected by malicious software, State of Alaska will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software (PCI Requirement 5.1.2).

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7 (PCI Requirement 5.2).

Steps must be taken to insure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period (PCI Requirement 5.3).

2.6 Requirement 6: Develop and Maintain Secure Systems and Applications

Not required for Dialup solutions.

2.6.1 Risk and Vulnerability

State of Alaska will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data (PCI Requirement 6.1).

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months) (PCI Requirement 6.2).

2.7 Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

2.7.1 Limit Access to Cardholder Data

Access to State of Alaska's cardholder system components and data is limited to only those individuals whose jobs require such access (PCI Requirement 7.1).

Access limitations must include the following:

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities (PCI Requirement 7.1.2).
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control) (PCI Requirement 7.1.3).

2.8 Requirement 8: Assign a Unique ID to Each Person with Computer Access

Not required for Dialup solutions.

2.8.1 Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties (PCI Requirement 8.3).

2.8.2 Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use (PCI Requirement 8.1.5).

2.9 Requirement 9: Restrict Physical Access to Cardholder Data

2.9.1 Physically Secure All Areas and Media Containing Cardholder Data

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel (PCI requirement 9.1.2).

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:
All media must be physically secured (PCI requirement 9.5).

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include (PCI Requirement 9.6):

- Media must be classified so the sensitivity of the data can be determined (PCI Requirement 9.6.1).
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked (PCI Requirement 9.6.2).
- Management approval must be obtained prior to moving the media from the secured area (PCI Requirement 9.6.3).

Strict control must be maintained over the storage and accessibility of media containing cardholder data (PCI Requirement 9.7).

2.9.2 Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons (PCI requirement 9.8).

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed (PCI requirement 9.8.1.a).

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel (PCI requirement 9.8.1.b).

Protection of Payment Devices
Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted (PCI requirement 9.9).

State of Alaska must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following (PCI requirement 9.9.1):

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) (PCI requirement 9.9.2).

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following (PCI requirement 9.9.3):

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

2.10 Requirement 10: Regularly Monitor and Test Networks

Not required for Dialup solutions.

2.10.1 Audit Log Collection

State of Alaska will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges (PCI Requirement 10.2.2).
- All invalid logical access attempts (failed logins) (PCI Requirement 10.2.4).
- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges (PCI Requirement 10.2.5).

State of Alaska's log generating and collecting solution will capture the following data elements for the above events:

- User identification (PCI Requirement 10.3.1).
- Type of event (PCI Requirement 10.3.2).
- Date and time (PCI Requirement 10.3.3).
- Success or failure indication (PCI Requirement 10.3.4).
- Origination of event (PCI Requirement 10.3.5).
- Identity or name of affected data, system component, or resource (PCI Requirement 10.3.6).

2.10.2 Audit Log Review

State of Alaska's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate (PCI Requirement 10.6.1):

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment (PCI Requirement 10.6.2).

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process (PCI Requirement 10.6.3).

State of Alaska must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup) (PCI Requirement 10.7).

2.11 Requirement 11: Regularly Test Security Systems and Processes

Not required for Dialup solutions.

2.11.1 Testing for Unauthorized Wireless Access Points

At least quarterly, State of Alaska will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment (PCI Requirement 11.1).

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.
  To facilitate the detection process, State of Alaska will maintain an inventory of authorized wireless access points including a documented business justification (PCI Requirement 11.1.1).

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10) (PCI Requirement 11.1.2).

2.11.2 Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), State of Alaska will perform vulnerability scanning on all in-scope systems (PCI Requirement 11.2).

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all “high” vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year (PCI Requirement 11.2.1).

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year (PCI Requirement 11.2.2).

For both internal and external vulnerability scans, State of Alaska shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel (PCI Requirement 11.2.3).

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse (PCI Requirement 11.3.4).

For all in-scope systems for which it is technically possible, State of Alaska must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel (PCI Requirement 11.5.1).

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider) (PCI Requirement 11.5).

2.12 Requirement 12: Maintain a Policy that Addresses Information Security

2.12.1 Security Policy

State of Alaska shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data (PCI Requirement 12.1).

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment (PCI requirement 12.1.1).

Critical Technologies
State of Alaska shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage (PCI requirement 12.3).
These policies must include the following:

- Explicit approval by authorized parties to use the technologies (PCI Requirement 12.3.1).
- Authentication for use of the technology (PCI Requirement 12.3.2).
- A list of all such devices and personnel with access (PCI Requirement 12.3.3).
- Acceptable uses of the technologies (PCI Requirement 12.3.5).
- Acceptable network locations for the technologies (PCI Requirement 12.3.6).
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity (PCI Requirement 12.3.8).
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use (PCI Requirement 12.3.9).

Security Responsibilities
State of Alaska's policies and procedures must clearly define information security responsibilities for all personnel (PCI Requirement 12.4).

2.12.2 Incident Response Policy

The State Security Office (SSO) shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations (PCI requirement 12.5.3).

It is currently available at:
https://intranet.soa.alaska.gov/admin/SecurityPolicies/ISP151IncidentResponse.pdf

Incident Identification
Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident
The State Security Office (SSO) should be notified immediately of any suspected or real security incidents involving cardholder data:
No one should communicate with anyone outside of their supervisor(s) or the SSO or the Department of LAW about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the State Security Office or Department of LAW.

Document any information you know while waiting for the SSO to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

2.12.3 Incident Response Stages

(PCI requirement 12.10.1)
Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

2.12.3.1 Contain, Eradicate, Recover and perform Root Cause Analysis

1. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the State Security Office or the Department of LAW will work with legal and management to identify appropriate forensic specialists.
2. Eliminate the intruder's means of access and any related vulnerabilities.
3. Research potential risks related to or damage caused by intrusion method used.
4. Notify applicable card associations.
   Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978

MasterCard
Contact your merchant bank for specific details on what to do following a compromise. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

DiscoverCard
Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

4. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local authorities (if appropriate)

6. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected.

2.12.3.2 Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the State Security Office and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

2.12.4 Security Awareness

State of Alaska shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

2.12.5 Service Providers

State of Alaska shall implement and maintain policies and procedures to manage service providers (PCI requirement 12.8).

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2).
- Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3).
- Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4).
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity (PCI requirement 12.8.5).