NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 1 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

PURPOSE

This document explains credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Management is committed to these security policies to protect information utilized by the University in attaining its business goals. All employees are required to adhere to the policies described within this document.

SOURCE

Comptroller's Office
State of Arizona Accounting Manual
Payment card Industry Data Security Standard Program

SCOPE

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Northern Arizona University'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, version 3.2 revision 1.1, released January 2017. Should Northern Arizona University (NAU) 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 NAU to determine the appropriate compliance criteria and implement additional policies and controls as needed.

POLICY

COMPLIANCE AND RESPONSIBLITLIES

Requirement 1: Build and Maintain a Secure Network

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.

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.

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.

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.
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall.
- Ensure the firewall allows only established connections into the network and denies any inbound connections not associated with a previously established session.

Any mobile and/or employee-owned computers with direct connectivity to 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.

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

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.

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

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 3 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

- 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.

Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. NAU must insure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

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.
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system.
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure.
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 4 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

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.

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.

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use:

- 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.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable.

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.

- 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.

- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

Displaying PAN

NAU 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:

- 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.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, NAU will use strong cryptography and security protocols. These controls will be implemented as follows:

- 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) is not to be used as a security control for authentication or transmission.

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

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

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.

For systems considered to be not commonly affected by malicious software, NAU 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.

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.

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.

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability

NAU 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.

All critical security patches must be installed within 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).

Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

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

Limit Access to Cardholder Data

Access to NAU's cardholder system components and data is limited to only those individuals whose jobs require such access.

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control).

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

User Accounts

The following must be followed for all user accounts that have access to the system or systems that are part of the payment environment:

- Assign all users a unique ID before allowing them to access system components or cardholder data.

- Limit repeated access attempts by locking out the user ID after not more than six attempts.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 8 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

- Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

- If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

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.

User Authentication

In addition to assigning a unique ID for each user, ensure proper user-authentication management for non-consumer users (i.e.: employees and contractors) and administrators on all system components by employing at least one of the following methods to authenticate all users:

Passwords/phrases must meet the following:

- Require a minimum length of at least seven characters.

- Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

Change user passwords/passphrases at least every 90 days.

Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.

Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.

Remote Access

Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 9 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

- Incorporate multi-factor authentication for all non-console access into the cardholder data environment for personnel with administrative access.

- Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.

Document and communicate password/authentication policies and procedures to all users.

Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.

- Shared user IDs do not exist for system administration and other critical functions.

- Shared and generic user IDs are not used to administer any system components.

Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all appropriate personnel.

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure All Areas and Media Containing Cardholder Data

Appropriate facility entry controls must be used to limit and monitor physical access to systems in the cardholder data environment.

Using video cameras, access control mechanisms, or both, individual physical access to sensitive areas shall be monitored. Collected data shall be reviewed and correlated with other entries. This data shall be stored for at least three months, unless otherwise restricted by law.

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

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.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 10 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

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

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

Strict control must be maintained over the storage and accessibility of media containing cardholder data.

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons.

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed.

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

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.

NAU 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:

- 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.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 11 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

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).

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:

- 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).

Requirement 10: Regularly Monitor and Test Networks

Audit Log Collection

NAU 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
- All invalid logical access attempts (failed logins).
- 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.

Northern Arizona University's log generating and collecting solution will capture the following data elements for the above events:

- User identification.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 12 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

- Type of event.
- Date and time.
- Success or failure indication.
- Origination of event.
- Identity or name of affected data, system component, or resource.

Audit Log Review

NAU's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate:

- 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.

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

NAU 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).

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 13 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, NAU will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment.

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, NAU will maintain an inventory of authorized wireless access points including a documented business justification.

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).

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), NAU will perform vulnerability scanning on all in-scope systems.

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.

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.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 14 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

For both internal and external vulnerability scans, NAU 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.

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.

For all in-scope systems for which it is technically possible, NAU 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.

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).

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

NAU shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data.

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

Critical Technologies

NAU 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.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 15 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

These policies must include the following:

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

SECURITY BREACH RESPONSE

Security Responsibilities

NAU's policies and procedures must clearly define information security responsibilities for all personnel.

Incident Response Policy

NAU's ITS department shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

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, 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 Comptroller's Office and ITS department should be notified immediately of any suspected or real security incidents involving cardholder data:

- Contact the ITS Department to report any suspected or actual incidents. The ITS phone number should be well known to all employees and should page someone during non-business hours.
- No one should communicate with anyone outside of their supervisor(s) or the Comptroller's Office and the ITS Department about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Comptroller's Office.
- Document any information you know while waiting for the ITS Department 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.

Incident Response Policy

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.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. 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. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-01
	Section: 310-01
	Page 17 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

performed. That documentation can be found at https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

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

2. Alert all necessary parties. Be sure to notify:

   a. Merchant bank

   b. Local FBI Office

   c. U.S. Secret Service (if Visa payment data is compromised)

   d. Local authorities (if appropriate)

3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: www.ncsl.org

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Comptroller's Office will work with legal and management to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities.

6. Research potential risks related to or damage caused by intrusion method used.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 18 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Comptroller's Office and the ITS Department 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.

Security Awareness

NAU shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security.

Service Providers

NAU shall implement and maintain policies and procedures to manage service providers.

This process must include the following:

- Maintain a list of service providers.
- 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.
- Implement a process to perform proper due diligence prior to engaging a service provider.
- Monitor service providers' PCI DSS compliance status.
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-01**
	Section: 310-01
	Page 19 of 19
	Responsible office: Comptroller
	Origination date: 4/1/2017
Subject: Payment Card Security Policy	Effective date: 7/1/2017
	Revision date: 4/26/2019

RELATED INFORMATION

Comptroller's Office Policies

Policy 301-01

Policy 108

ITS Polices

https://nau.edu/its/policies/

Bank Card Merchant Security Requirements:

Visa U.S.A. Cardholder Information Security Program (CISP)

MasterCard International Site Data Protection (SDP) Program

American Express Data Security Standards (DSS)

Discover Information Security and Compliance (DISC) Program

Payment Card Industry (PCI-DSS) Standards

Payment Application Best Practices (PABP)

Arizona Revised Statute (A.R.S.) 44-7501 – Notification of Breach of Security System

Approved Service Providers:

PCI Security Standards Council Validated Payment Applications

Visa Global Registry of Service Providers