NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-02**
	Section: 310-02
	Page 1 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/22/2022

PURPOSE

This section outlines policies and procedures pertaining to the authorization granted to University departments and affiliates, hereon referred to as merchants, to accept bank/credit cards as a form of payment for services performed or for merchandise sold. Merchants are subject to and must comply with this policy and the guidelines in the exhibits to this policy.

SOURCE

Comptroller's Office
State of Arizona

SCOPE

Northern Arizona University departments that accept bank/credit/debit cards as a form of payment for services performed and/or merchandise sold.

DEFINITIONS

Acquiring Bank-Merchant bank contracted through Comptroller's Office on behalf of all University units and affiliates to perform bank card processing services.

Approved Scanning Vendor (ASV)-Approved Scanning Vendors (ASVs)_are organizations that have been approved by the Payment Card Industry Council that validate adherence to certain Payment Card Industry Data Security Standards requirements by performing external vulnerability scans of internet public facing environments of merchants and service providers.

Authorization-Process by which a merchant obtains prior confirmation from the acquiring bank that a specific financial transaction will be processed successfully when settlement is completed.

Bank/Credit Card- Unexpired credit card affiliated with a credit card company (e.g., Visa U.S.A., MasterCard International) or branded debit card, ATM cards, and any other card or device other than cash or checks affiliated with recognized banking networks for which a merchant has established card acceptance with the acquiring bank.

Bank/Credit Card Acceptance Fees/Charges-Costs imposed on merchants by the acquiring bank in exchange for the privilege of accepting a card. Discount fees are comprised of four components:

1. Bank Discount Rate Fee- Acquirer bank charge on all bank/credit card transactions for processing card sales and credits.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-02
	Section: 310-02
	Page 2 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

2. Interchange--non-negotiable fees established by the credit card associations which are collected from the merchant by the acquiring bank and paid by the acquiring bank to the issuing banks.
3. Assessments/Access--non-negotiable fees established by the credit card associations which are collected from the merchant by the acquiring bank and paid by the acquiring bank to the credit card associations.
4. Processor's fee--negotiable cost established by contract which is collected by the acquiring bank on their own behalf. Processor fees are negotiated and contracted through the Request for Proposal (RFP) process and Comptroller's Office.

Cardholder Information-Personally identifiable data associated with the cardholder including account number, expiration date, card validation number (e.g. CVV2, CVC2), transaction information or any other information that may be used to personally identify a bank card account or holder.

Campus Merchant Agreement-An agreement between Student and Departmental Account Services and the campus University merchant that outlines the responsibilities, rules, regulations and contractual provisions and obligations regarding the handling of bank/credit cards. The agreement must be signed by the head of the unit that is providing the option of accepting bank/credit cards to sell goods and services to their customers.

Centralized Payment Process-Controlled system of Internet sites, software applications, and communication protocols that interact together for the purpose of capturing and transferring cardholder information to the acquiring bank via the Internet and securely storing the information in a single repository, commonly known as a "gateway".

Chargeback - A reduction of the merchant's cash receipts initiated by the acquiring bank in response to a transaction that has been rejected by the acquiring bank, issuing bank or disputed by the cardholder.

E-Commerce-Website based business transaction utilizing electronic payments such as bank/credit cards.

Student and Departmental Account Services -A team of Comptroller Office personnel who provide services, information, merchant account set up, and act as a liaison between the Acquiring Bank and the Merchant Units.

Issuing Bank – Financial institution that grants credit to a cardholder by issuing a credit card to the cardholder.

Merchant Unit / Merchant Department-A University department or an affiliate of the University that has received the appropriate prior authorization to accept cards as a form of payment for services performed or for merchandise sold by the department or affiliate. A merchant is assigned a

specific merchant account(s) with the acquiring bank. Merchants fall into one of the following three categories:

1. Retail merchant--conduct the entire card transaction in a face-to-face environment with the card physically present for the transaction.
2. Phone/mail merchant--generate cardholder information forms either through telephone communication with the cardholder, through the mail, or by standalone facsimile machine not connected to any computer network.
3. Internet merchant (E-Commerce)--conduct all of their card transactions through the Internet within the centralized payment process.

Merchant Account - A unique account established with the acquiring bank that is used to track equipment, transactions, fees, compliance activities, and designated points of contact and all related information of the merchant.

Merchant Responsible Person (MRP) - A unit's designated individual within that merchant unit who will have primary authority and responsibility for Payment Card Industry Data Security Standards (PCI-DSS) documentation for bank card transaction processing.

Operating Guidelines - Rules and procedures published by the acquiring bank that specify the operational parameters that each merchant must adhere to when accepting a card as a form of payment.

PCI-DSS -- Payment Card Industry Data Security Standards - A specific set of technical requirements and business practices published collaboratively by Visa U.S.A. and MasterCard International addressing cardholder information security that each merchant must comply with and demonstrate compliance on a periodic basis. (e.g., Visa U.S.A. Cardholder Information Security Program (CISP), MasterCard International's Site Data Protection Program (SDP), American Express's Data Security Standards (DSS) and Discover's Information Security and Compliance (DISC) Program).

Qualified Security Assessor (QSA) -The Payment Card Industry (PCI) QSA designation is conferred by the PCI Security Standards Council to individuals that meet specific information security education requirements. The primary goal of QSA is to complete PCI compliance assessments, auditing and consulting for merchants to ensure and validate the merchant is meeting PCI standards.

S**ettlement -** Process by which a merchant presents a single or group of financial transactions to the acquiring bank for the purpose of converting the credit information collected from a cardholder into cash receipts.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-02**
	Section: 310-02
	Page 4 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

POLICY

CMP 310-02: Accepting Credit Cards as a Form of Payment

1. Per Arizona Board of Regents 3-102, the responsibility for the collection of monies in connection with University activities is delegated to the Associate Vice President for Financial Services / Comptroller, who, in turn, delegates this responsibility to the Student Department and Account Services (SDAS) office. SDAS should be contacted regarding any deviations from policies and procedures stated herein.

2. Only the Comptroller's Office has the delegated authority to execute agreements on behalf of the University in connection with banking-type services and regulate the use of bank/credit card services.

3. Services for processing bank/credit cards, depositing cash receipts and any specialized programs or services (e.g. shopping carts, electronic check payment, third party applications) that process directly or have the ability to authorize bank/credit card transactions for payment of University sales and services must have written permission from the Comptroller's Office. Merchants may use only service providers, approved by Contracts, Purchasing, and Risk Management, and the Comptroller's Office, that meet payment card and acquiring bank certifications, regulations and requirements.

4. Merchants are required to use a Point-to-Point Encryption Technologies (P2PE) device established through the PCI DSS Security Council. All in use devices must be listed on the Comptroller's Office list of approved devices. With the Comptroller's Office and Cash Management Office approval through consultation with the NAU Chief Information Officer, other PCI DSS validated P2PE solutions may be adopted to support unique merchant payment processing requirements. Alternatives to the preferred solution may bring more risk to NAU, and therefore will be highly scrutinized.

5. Merchants must agree and adhere to all federal, bank/credit card regulations, payment card industry (PCI) data security standards, and University policies and standards, including without limitation the Information Security Policy and the standards and procedures established under it, in the acceptance, processing, and storing of bank/credit card transactions as outlined in the "Merchant Bank/credit Cards Acceptance Agreement" and the PCI standards located online at https://www.pcisecuritystandards.org/

6. Merchants may not accept bank/credit cards or authorize or complete settlement for transactions of other University department/units or affiliates without written authorization from the Comptroller's Office.

7. Bank/credit cards may be accepted by a merchant for University gifts and donations. The merchant must contact the NAU Foundation for the specific processes to report the donations and/or gifts.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-02**
	Section: 310-02
	Page 5 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

8. A merchant that plans to receive revenue from external sales or services and provide taxable goods to customers outside the University should contact the Comptroller's Office to discuss sales tax requirements. Merchants should also refer to and be familiar with Policy CMP 108 and Policy CMP 120.

9. Merchants that accept bank/credit cards and/or electronic payments for gifts, goods or services must designate a full time University employee who will have primary authority and responsibility for department/unit compliance of ecommerce and bank/credit card transaction processing. This individual will be referred to in the remainder of this policy statement as the Merchant Responsible Person. All Merchant Responsible Persons will be responsible for the department/unit complying with all security measures established by the payment card industry, the NAU Information Security Office, the "Merchant Bank/Credit Cards Acceptance Agreement" and this policy.

10. Merchant's must review and sign the "Merchant Bank/Credit Cards Acceptance Agreement" upon their request for merchant status. With their signature, the department/ unit's head and Merchant Responsible Person acknowledge that they understand and agree with the terms and responsibilities outlined in the agreement. This agreement must be renewed annually.

11. No University employee, contractor or agent who obtains access to bank/credit card or other personal payment information in the course of conducting University business may sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes or other media obtained by reason of a card transaction to any third party other than to University's acquiring bank, depository bank, Visa, MasterCard or other bank/credit card company or pursuant to a government request. All requests to provide information to any party outside of the merchant must be coordinated with the Comptroller's Office, ITS and Institutional Research and Analysis.

12. Merchant must use a University authorized service provider to process all e-commerce transactions or web based transmissions of transactions. If a department believes that it has a significant business case or processing requirement that cannot be achieved using an authorized service provider and wishes to utilize an alternative, it must initiate a written request to the Comptroller's Office for approval of use. The Comptroller's Office will review the request with Contracting, Purchasing, and Risk Management and notify the department of approval or rejection of service provider use. If approved, the department and service provider are responsible to meet all PCI-DSS requirements and documentation.

13. If the merchant chooses not to utilize the provided ecommerce gateway and an alternative ecommerce gateway or software is necessary, the gateway and service provider must be included on either the Visa Global Registry of Service Providers, or PCI Security Standards Council List of Validated Payment Applications. In addition, the alternative service provider must also be approved by the acquiring bank, the Comptroller's Office and Contracting, Purchasing, and Risk Management. The third party service provider must also comply with all University policies.

NAU NORTHERN ARIZONA UNIVERSITY	POLICY: CMP 310-02
	Section: 310-02
	Page 6 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

14. All service providers that share cardholder data or that could affect the security of the cardholder data must sign an agreement that outlines the security responsibilities of the service provider and the University. The service provider must agree to provide information requested from the University or its PCI Qualified Security Assessors to verify security due diligence and PCI-DSS compliance.

15. All ecommerce websites that redirect or link to an authorizing gateway must perform quarterly external vulnerability scans through a PCI approved scanning vendor (ASV) and annual internal scans through University provided applications. External scans must be performed after significant network or website changes. All vulnerabilities ratings of four or more must be resolved within 30 days and rescanned until passing results are achieved.

16. Upon request of the Comptroller's Office, the merchant will complete annual PCI-DSS Self-Assessment Questionnaire and supporting documentation including network security scans deemed necessary by ITS, Comptroller's Office, or payment card industry. The merchant will be responsible for the costs of such service. The service will include assistance to the merchant in understanding and completing the Self-Assessment Questionnaire.

17. A Merchant's ability to offer bank/credit card payment is conditioned on compliance with the PCI-DSS. The merchant is responsible for complying and maintaining PCI-DSS standards. If the merchant fails compliance, the merchant is responsible for correcting deficiencies to bring the merchant into compliance as directed by the Comptroller's Office. Failure to comply with PCI- DSS standards will result in withdrawal of the merchant's ability to accept bank/credit cards.

COMPLIANCE AND RESPONSIBILITIES

The Comptroller's Office is responsible for:

a. Reviewing and initiating requests from University departments and affiliates to establish a merchant account and accept bank/credit cards as a form of payment for services performed or for merchandise sold by such units and affiliates.

b. Providing information and assistance to University departments and affiliates that are analyzing the responsibilities and costs of accepting bank/credit cards as a form of payment.

c. Selecting and ordering terminals and other equipment and coordinating all compliance activities for the merchant.

d. Coordinating all merchant compliance activities that are required or directed by University policies, payment card industry, Information Technology Services, and acquiring bank standards.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-02**
	Section: 310-02
	Page 7 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

All merchants are responsible for:

a) Following security measures established by the payment card industry, ITS and Comptroller Office policies.

b) Performing all periodic compliance activities requested by ITS in coordination with the Comptroller's Office in a timely manner.

c) Recording all card transactional activity on the general ledger within three business days of settlement.

d) Reviewing monthly merchant statements for accuracy. Inaccurate charges must be reported to the Comptroller's Office within 60 days of statement date.

e) Notifying the Comptroller's Office immediately when accounts are no longer needed and should be deactivated.

f) Responding to chargeback notifications and bank Card Company inquires within chargeback notification letter deadlines.

g) Insuring that no cardholder information is stored electronically in any database, application, fax machine or system.

h) Following the responsibilities and guidelines in the exhibits included within this policy.

SECURITY BREACH RESPONSE

1. All suspected and/or confirmed security compromises must be reported immediately to ITS and the Comptroller's Office.

2. If a security breach is confirmed by ITS and the Comptroller's Office, the Comptroller's Office will be responsible for alerting the merchant acquiring bank, the payment card associations and other merchant regulatory entities deemed necessary of the confirmed security breach. The ITS Office will be responsible for providing the security breach information to all government agencies required by statute.

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 310-02**
	Section: 310-02
	Page 8 of 8
	Responsible office: Comptroller
	Origination date: 04/01/2017
Subject: Accepting Credit Cards as a Form of Payment	Effective date: 07/01/2017
	Revision date: 04/26/2019

RELATED INFORMATION

Comptroller's Office Policies

- Policy 301-01
- Policy 310-01
- 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