COMPTROLLER POLICY MANUAL

NAU NORTHERN ARIZONA UNIVERSITY	**POLICY: CMP 110-01**
	Section: 100 General
	Page **1** of **2**
	Responsible office: Comptroller
	Origination date: 02/01/2008
Subject: Payment Card Compliance	Effective date: 02/01/2008
	Revision date: 02/26//2016

PURPOSE

To provide the university with clear and manageable steps to protect customer cardholder data and to protect the university from a cardholder breach by complying with Payment Card Industry (PCI) Data Security Standards (DSS)

SOURCE

PCI Compliance
University policy

APPLICABILITY

Required for those who handle, process, support, and manage payment card transactions received by the university to comply with the current version of the PCI DSS.

POLICY

CMP 110-01 PCI Compliance

For a list of definitions please visit the PCI Security Standards PCI DSS Glossary.

This policy sets the requirements for all University departments that accept credit cards using a payment card terminal as well as those processing or sending transactions using e-Commerce.

1) Terminal transactions include face-to-face transactions via phone line or cellular terminals. In some cases, a terminal's keypad may be used to enter card-not present transactions where cardholder data was received via postal mail or over the phone.

2) e-Commerce transactions include the following:
    a. Links on university websites redirecting customers to another payment website;
    b. IP-connected terminals processing payments on the Internet;
    c. Point of sale transactions at a computer cash register using PCI payment applications including point of sale software on a computer to transmit, process, or store cardholder data;
    d. Use of third party vendor's virtual payment terminal to transmit, process, or store cardholder data; or
    e. Transactions transmitted, processed and stored on the university network.

3) This policy requires each University department to use pre-approved payment processing methods. Please contact Information Technology Services for help determining that proper payment processing methods are followed.

4) University departments using third party vendors must comply with the current PCI regulations and university PCI requirements.

5) All departments must consult with Contracting and Purchasing Services (CPS) when purchasing any type of technology that accepts credit card payments. CPS will be responsible for adding standard PCI language to all contracts.

It is the responsibility of all individuals to whom this policy applies to be informed of and follow the requirements under this policy and any associated documents to protect cardholder data.

Employees who violate this policy may be subject to disciplinary action, including and not limited to termination of employment and/or potential criminal prosecution under applicable federal, state and local laws.

Other individuals to whom this policy applies who violate this policy are subject to appropriate sanctions, including but not limited to termination of the relationship and/or potential criminal prosecution under applicable federal, state, and local laws.

CROSS-REFERENCES

PCI Security Standards Council

PCI Compliance Guide