
# PAYMENT CARD PROCEDURE

**Prepared by**

**Controller's Office**

**April 2026**

# College of Southern Nevada
# Payment Card Procedures

### Payment Card Industry Data Security Standards (PCI DSS)

## Purpose

This document and additional supporting documents represent the College of Southern Nevada's procedures to reduce the chance of loss/disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in monetary loss for customers, suspension of payment card processing privileges, and fines imposed on, and damage to the reputation of the unit and the organization.

## PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) is a mandated set of requirements agreed upon by the six major credit card companies: VISA, MasterCard, Discover, American Express, JCB, and UnionPay. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept credit and debit cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council (PCI SSC) website (https://www.pcisecuritystandards.org).

In order to accept payment cards, the College of Southern Nevada must maintain compliance with the PCI DSS at all times. Merchants must also assess/attest compliance status annually and, if found to be non-compliant at any time, must be actively working toward compliance in accordance with methodology and conditions set by their merchant services provider(s). The College of Southern Nevada's Payment Card Procedure and additional supporting documents provide the requirements for processing, transmitting, storage, and disposal of payment card data. This is done to reduce the organizational risk associated with the acceptance of card payments by individual departments and to ensure proper internal control and compliance with the PCI DSS.

## Scope/Applicability

The College of Southern Nevada Payment Card Procedures applies to all individuals, systems, networks, faculty, staff, contractors, students, consultants, organizations, and third-party vendors involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of the College of Southern Nevada. Purchasing Card (aka P-Card) data does not fall under the PCI DSS requirements, but shall be protected in a similar manner, particularly as it relates to storage and disposal of cardholder data (CHD).

# Authority

The Institution President or his/her designee will direct the development and implementation of the College of Southern Nevada's policies and procedures.

# Procedures

In the course of doing business at the College of Southern Nevada, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. The College of Southern Nevada requires all departments that accept payment cards to do so only in accordance with PCI DSS requirements and the following procedures.

## 1. Card Acceptance and Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards is approved on a case-by-case basis. Any fees associated with the acceptance of the payment card in that department may be charged to the individual department.

1.1. Interested departments or merchants should contact the Controller's Office to begin the process of accepting payment cards. Steps include:
   1.1.1. Attain written approval from the Dean or Associate Vice President.
   1.1.2. Written approval from the Controller.
   1.1.3. Completion of training
   1.1.4. Review and acknowledgement of all relevant policies for payment card processing and security

1.2. Any department accepting payment cards on behalf of the organization or related entities must designate an individual within the department who will have primary authority and responsibility within that department for payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.

1.3. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established and are also available by contacting the Controller's Office.

1.4. Departments may only utilize service providers, third parties, solutions, platforms, and equipment approved by the Controller's Office. If a department believes that existing, approved solutions do not meet its customer service requirements, the department must meet with the Controller's office to discuss alternative options before moving forward with another solution. Do not begin formal procurement steps prior to meeting with the Controller's office and receiving approval for the new company/software.

1.5. All service providers and third-party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:
    1.5.1. Ensure contracts include language stating that the service provider or third-party vendor is PCI compliant, takes responsibility for sensitive data it processes, stores, or interacts with on behalf of the organization, and will properly protect such data.
    1.5.2. Collect an Attestation of Compliance (AOC) and PCI responsibility matrix from the third party prior to establishing the relationship, as part of due diligence.
    1.5.3. Annually confirm the PCI compliance status of all service providers and third-party vendors by ensuring that valid AOCs (covers the service(s) being used and is less than one year old since signature date) are received and responsibility matrixes are refreshed. A lapse in PCI compliance could result in the termination of the relationship.

## 2. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

***PROCESSING AND COLLECTION***

2.1. Access to payment card data (cardholder data [CHD] plus sensitive authentication data [SAD]) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD/SAD and review the list quarterly to ensure that the list reflects the most current access needed and granted.
2.2. Equipment used to collect/process cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:
    2.2.1. Maintaining an inventory/list of devices and their locations.
    2.2.2. Inspecting the devices to check for signs of tampering or substitution on the first day of the work week.
    2.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.
2.3. Email and similar end-user messaging must never be used to accept payment card data. Please refer to the Payment Card Procedure for required responses/actions.
2.4. Fax machines used to receive payment card information must be standalone machines, connecting to analog telephone lines, and with appropriate physical security; receipt or transmission of payment card data using a multi-function fax machine or cloud fax integrated with email is not permitted.

***STORAGE AND DESTRUCTION***

2.5. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access throughout its lifecycle.
2.6. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.
2.7. Departments may never store any CHD in any electronic format, as this removes eligibility for any shortened Self-Assessment Questionnaires (SAQs). Merchants are never permitted to retain SAD, in any format, once authorization is complete. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card validation code.
2.8. CHD must not be retained any longer than that defined by a legitimate business need. CHD must be destroyed immediately after processing or after the required retention period, using a PCI DSS-approved method of destruction. Refer to the Payment Card Procedure for specific requirements related to retention of CHD.

## 3. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the department's network and processing environment are analyzed. PCI DSS scope includes all people, processes, and technologies that interact with or affect the security of payment card data.

## 4. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the College of Southern Nevada Payment Card Incident Response Plan. The plan must include notifications, staff requirements, and response procedures, as well as card brand contact strategies. If the suspected activity involves computers (e.g., hacking, unauthorized access, etc.), immediately notify the Chief Information Office and VP of Finance and Administration.

## 5. Procedure and Training

Ensure documentation governing payment card data exists and that it covers the entirety of the PCI DSS. Ensure that roles and responsibilities for performing activities related to PCI DSS Requirements are documented, assigned, and understood, as appropriate for assigned SAQs. Document users' acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.