

**Payment Card Industry (PCI) Compliance POLICY**

**Summary**

The Payment Card Industry Data Security Standard (PCI DSS) is a mandated set of requirements agreed upon by the major credit card companies. The security requirements apply to all transactions surrounding the payment card industry and the merchants or organizations that accept these cards as a form of payment.

**Purpose**

The purpose of the policy is to provide guidance about the importance of protecting payment card data and customer information. Failure to protect this information may result in financial loss for customers, suspension of credit card processing privileges, fines, and damage to the reputation of the college.

**Policy Statement**

Western Nevada College is committed to compliance with the PCI DSS to protect payment card data regardless of where that data is processed or stored. Payment card data includes primary account numbers, cardholder name, expiration date, service code, and sensitive authentication data. All members of the college community must adhere to these standards to protect our customers and maintain the ability to process payment using payment cards.

The college prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any college system, database, USB drive, network, computer, tablet, cell phone, or paper file. Storing truncated numbers, in approved formats (first six digits or last four digits) is permissible.

The college prohibits anyone to send or request cardholder information to be sent via email, fax, instant messaging, chat, etc. If a staff member receives payment card information in this manner, take it immediately to the cashier to complete the transaction and immediately delete the message.

A list of credit card terminals, including make and model of the device, physical location, and serial number, will be maintained by the Controller’s Office. Cashiers and other departmental personnel with access to the terminals will periodically inspect terminal for possible tampering or substitution and report suspicious behavior and indications of possible device tampering or substitution to appropriate personnel.

**Scope**

WNC maintains a limited card processing environment. Card payments are limited to:

* Ecommerce transactions through:
  + The Student Self-Service Payment Center
  + Western Nevada Musical Theatre Company Payment Center
  + WNC Continuing Education Payment Center
* In-person or via telephone transactions through stand-alone payment terminals
  + Carson Cashier’s Office
  + Fallon Cashier’s Office
  + Child Development Center

All employees or other designated individuals who collect, maintain, or have access to credit card information or credit card terminals must comply with the PCI policy and complete annual PCI Training. Others who do not have access but accidentally gain access must report that information to his or her supervisor immediately.

**Standards**

The Chart details the acceptable use of payment card and security requirements. The PCI DSS requirements do not supersede local, state, and federal laws or regulations.

**Payment Card Industry Data Security Standards (PCI DSS) V4**

|  |  |
| --- | --- |
| **Goals and PCI DSS Requirements** | |
| **Goals** | **PCI DSS Requirements** |
| Build and Maintain a Secure Network and Systems | 1.  Install and Maintain Network Security Control  2.  Apply Secure Configurations to All System Components |
| Protect Cardholder Data | 3.  Protect Stored Account Data  4.  Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks |
| Maintain a Vulnerability Management Program | 5.  Protect all Systems and Networks from Malicious Software  6.  Develop and Maintain Secure Systems and Software |
| Implement Strong Access Control Measures | 7.  Restrict Access to System Components and Cardholder Data by Business Need to Know  8.  Identify Users and Authenticate Access to System Components  9.  Restrict Physical Access to Cardholder Data |
| Regularly Monitor and Test Networks | 10. Log and Monitor All Access to System Components and Cardholder Data  11. Test Security of Systems and Networks Regularly |
| Maintain an Information Security Policy | 12. Support Information Security with Organizational Policies and Programs. |

For more information about the standard [visit the official PCI Security website](https://east.pcisecuritystandards.org/).