SECTION #: 1.0 GENERAL

SUBJECT: PCI DSS COMPLIANCE

Background: All LC State departments that process or transmit payment cardholder data must adhere to Payment Card Industry Data Security Standard (PCI-DSS) requirements. Compliance is mandatory to ensure the security of financial transactions and protect sensitive data from unauthorized access or breaches.

Point of Contact: Vice President for Finance and Administration and Director of Information Technology

Other LC State offices directly involved with implementation of this policy, or significantly affected by the policy: All departments that accept credit card payments

Date of approval by LC State authority: April 7, 2026

Date of State Board Approval: N/A

Date of Most Recent Review: April 7, 2026

Summary of Major Changes incorporated in this revision to the policy: This is a new policy

1. Policy

The purpose of this policy is to establish guidelines for ensuring compliance with the Payment Card Industry Data Security Standard (PCI-DSS). Lewis-Clark State College (LC State) is committed to protecting cardholder data and maintaining the security of all financial transactions involving payment card information. LC State allows transmissions of Cardholder Data over wired networks and secured wireless networks. LC State also does not allow the storage of Cardholder Data on its network devices. This policy defines the roles, responsibilities, and security measures required to achieve and maintain PCI-DSS compliance.

2. Definitions

A. Cardholder Data (CHD): Information associated with a payment card, including the primary account number (PAN), cardholder name, expiration date, and service code.

B. Sensitive Authentication Data (SAD): Security-related data used for authentication (e.g., full track data, PINs, CVV codes), which must not be stored after transaction authorization.

C. Cardholder Data Environment (CDE): The systems and processes involved in storing, processing, or transmitting CHD.

D. Multi-Factor Authentication (MFA): A security process that requires multiple verification methods before granting access.

E. **Encryption**: The process of converting information into a secure format to prevent unauthorized access.

3. Compliance Requirements

LC State must comply with the following PCI-DSS requirements

A. Build and Maintain a secure Network and Systems
   i. Implement network security controls (firewalls, segmentation).
   ii. Change default passwords and security settings before deploying systems.
   iii. Conduct periodic reviews of firewall and network security configurations.

B. Protect Cardholder Data
   i. Encrypt CHD during transmission over public networks.
   ii. Do not store SAD after transaction authorization.
   iii. Perform annual reviews of encryption protocols and data protection measures.

C. Maintain a Vulnerability Management Program
   i. Deploy and maintain anti-malware and intrusion detection systems.
   ii. Regularly update software and apply security patches.
   iii. Conduct monthly vulnerability scans and remediate identified issues.

D. Implement Strong Access Control Measures
   i. Restrict access to CHD based on a business need-to-know basis.
   ii. Require individual logins and do not use shared departmental accounts.
   iii. Enforce strong password policies.
   iv. Conduct quarterly access control reviews and revoke unnecessary access.

E. Regularly Monitor and Test Networks
   i. Log all access to system components handling CHD.
   ii. Conduct quarterly vulnerability scans and annual penetration tests.
   iii. Perform periodic log reviews to detect unauthorized activity.

F. Maintain an Information Security Policy

i. Establish and enforce a formal security awareness program.

ii. Implement an incident response plan for security breaches.

iii. Conduct annual security training for all employees handling CHD.

4. Roles and Responsibilities

A. Director of Information Technology
   i. Oversees PCI-DSS compliance and security controls.

B. Finance and Administration
   i. Ensures payment processing procedures comply with PCI standards.

C. All Employees Handling CHD
   i. Must follow PCI-DSS policies, complete security training, and report potential security incidents.

5. Enforcement and Penalties

A. Failure to comply with this policy may result in disciplinary action, loss of payment processing privileges, or legal consequences. Violations must be reported to the Director of Information Technology for investigation.

6. Review Committee

A. A committee shall be formed to review and update the policy as necessary. The committee shall include representatives from both the Information Technology and Finance Departments along with other key stakeholders.

7. Policy Review and Updates

A. This policy will be reviewed annually or as necessary to reflect updates to PCI-DSS requirements. Revisions must be approved by LC State's Information Technology and Finance departments.