65-9 Payment Card Security

65-8-1 Purpose • 65-8-2 Policy • 65-8-3 Administration • 65-8-4 Definitions
65-8-5 Payment Card Security Procedures • 65-8-6 Plan Administration • 65-8-7 Periodic Reviews

1. **Purpose.** The purpose of this policy is to outline Eastern New Mexico University System (the System) credit and purchasing card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. The System's *Payment Card Security Procedures Guidelines* provides operationalizes this policy.

2. **Policy.** This policy specifies the PCI requirements that apply to all the System's campuses and units that store, process, or transmit cardholder data to protect consumers, reduce risk from identity fraud and minimize potential damage to the System from fraud or misuse. This is accomplished by meeting PCI requirements for all units that store, process or transmit cardholder data and complying with the Payment Card Industry Data Security Standard (PCI DSS) 3.2 program and all subsequent updates and regulations. Elements of compliance include the following:

   A. To build and maintain a secure network, systems and applications for the System and its business transactions (PCI requirements 1, 6); and to regularly update anti-virus software (PCI requirement 5)

   B. To protect stored cardholder data and to encrypt cardholder data transmitted across open, public networks (PCI requirements 3, 4);

   C. To appropriately restrict access to cardholder data by businesses on a need-to-know basis (PCI requirement 7);

   D. To assign unique IDs to each person with computer access to network systems and applications and to avoid use of vendor-supplied defaults for system passwords or other security parameters (PCI requirements 2, 8);

   E. To restrict physical access to cardholder data (PCI requirement 9) by securing all areas and media containing cardholder data, appropriately destroying data when no longer needed, and to assure the security of all devices that capture cardholder information;

   F. ENMU tracks and monitors all access to network resources and cardholder data (PCI requirement 10);

   G. To regularly monitor and test security systems and processes and maintain a policy that addresses information security for employees and contractors (PCI requirements 11, 12).

The forgoing policies, procedures and Plan shall be implemented using the following:

Guidelines and Procedures

3. **Administration.** This policy and the associated Payment Card Security Procedures Guidelines shall be jointly administered by the ENMU System chief financial officer (CFO) or his/her designee and the ENMU System chief information officer (CIO).

4. Definitions.

A. “Cardholder data” is all identifiable personal data about the cardholder and the relationship to the client. Cardholder Data includes but is not limited to name, address, account number or portion of an account number, expiration date, full track 1 and/or 2 data, PIN, mag stripe data, and Card Verification Value (CVV), the three-digit check number encoded on the magnetic stripe or Card Verification Value 2 (CVV2), the three-digit value printed on the back of many major credit cards).

B. “Incident.” For purposes of this policy, refers to an event of a known or suspected data compromise or breach.

5. Payment Card Security Procedures

A. Oversight. The Payment Card Security procedures, specified under PCI DSS, are administered by the CFO for business transactions and the CIO for network and system security. All ENMU System units that wish to process credit/debit card payments must be approved through the Business Office.

B. Security Responsibilities

1. **Employee Responsibility**. Eastern New Mexico University System policies and procedures shall clearly define information security responsibilities for all personnel. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility.

   Employee Training. The CIO shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations and assure that employees in the unit receive regular training in maintaining system and network security. The CFO shall establish employee-training procedures so that all employees are aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures.

2. **Reporting an Incident.** Any employee suspecting or detecting a breach in the network or system or a violation or possible violation of security protocols should immediately report this to his/her supervisor or executive administrator. The CIO and the CFO shall be notified immediately of any suspected or real security incidents involving cardholder data.

   The CIO and the CFO shall contact the chief of The Department of Public Safety to report any suspected or actual incidents and notify the Internal Auditor.

   Employees should not communicate with anyone outside of their supervisor(s) or designated emergency contact about any details or generalities surrounding any suspected or actual incident. The branch community college president or the chancellor will coordinate all communications with law enforcement or the public.

3. **Incident Response Procedure.** Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

4. **Responses to Incidents**. The following protocols will be employed in the event of an incident or system breech:

a. Internal. In the event of an internal breach of security or violation of policy or procedure by one or more employees or units, the CFO or his/her designee shall notify all appropriate personnel and take steps to mitigate the breach or violation of policy or procedure.

b. External. In the event of an external breach of network or system or a detected security breach in campus systems, the CIO or his/her designee shall notify all appropriate personnel and take steps to mitigate the breach.

c. Specific protocols for addressing security breaches are addressed in the Payment Card Security Procedures Guidelines.

6. Plan Administration.

A. **Training Oversight.** The CFO or his /her designee is responsible for ensuring appropriate training of all employees in required PCI business transaction practices and prompt response to breaches or potential breaches of the system. The administrator shall direct that periodic reviews of the Plan be conducted as needed for updates and improvements.

B. **System Security Oversight.** The CIO or his/her designee is responsible for ensuring training for network personnel to secure networks and systems, monitoring operations, and responding promptly to breaches or potential breaches of the secure system.

C. **Non-Disclosure of Specific Practices**. Knowledge about specific security protocols, breach identification, detection, mitigation and prevention practices may need to be limited to employees or personnel on a need to know basis. Documents produced or developed that describe such specific practices are considered confidential and should not be shared with other System employees or the public.

7. Periodic Reviews. The System shall maintain and periodically update its Payment Card Security Procedures Guidelines, business and technology protocols and this policy assure the security of credit card or purchasing card information, in compliance with PCI DSS.

Approved by Board of Regents, March 11, 2016.
Approved by Board of Regents, June 1, 2019