Title: Payment Card Services

Related Policy and Procedures:

Division of Responsibility: Business and Administrative Services; Institutional Research, Planning, Effectiveness and Technology

Credit card processing at the College shall comply with the Payment Card Industry Data Security Standards (PCI DSS). The following security requirements have been established by the payment card industry and adopted by the College to ensure compliance with the payment card industry. These requirements apply to all employees, systems and networks involved with credit card processing, including transmission, storage or electronic and paper processing of credit card numbers.

I. AUTHORIZED EMPLOYEES

Credit card processing for official college business is restricted to authorized personnel only. No other College employees are authorized to process such information for any reason. College employees who process credit card information or who have access to this information will complete annual data security training.

II. PROCEDURES

A. Each College employee who processes credit card information must strictly adhere to the following:

1. Access to credit card information is restricted to authorized personnel.

2. System and desktop passwords must be regularly changed.

3. Accounts should be immediately terminated or disabled for employees who leave employment with the College.

4. Credit card information in transit must be securely stored until processed.

5. Credit card information must not be stored in any format after processing.

B. Credit card information, including the card number, cardholder name, CVV code and expiration date should not be retained for any reason.

C. Employees may not send or process credit card data in any insecure manner including transmitting such data via email, or instant messaging. Credit card information may not be left exposed to anyone.

D. The College's Information Technology Department shall maintain additional procedures to ensure compliance with PCI DSS including:

1. Configuration of card processing procedures, including segmentation of local area networks and protection through deployment of firewalls.

2. Logging control procedures.

3. Wireless use procedures.

4. Encryption procedures.

Legal Reference: N.C. Community College Written Memoranda CC10-029 (issued 7/21/10)

June 13, 2023	June 13, 2023	N/A
Date Approved by Board of Trustees	**Date of Last Review**	**Date of Last Revision**