# CENTRAL CAROLINA COMMUNITY COLLEGE
# POLICY & PROCEDURE MANUAL

**Financial Services Section**

*Policy 6.3.8 - Payment Card Security*

**I. AUTHORIZED INDIVIDUALS......................................................................................1**
**II. PROCEDURES.....................................................................................................1**

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 INDIVIDUALS

Credit card processing for official college business is restricted to Business Office personnel and other individuals so authorized by the President or the Chief Financial Officer. 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.

Students may also be authorized to process credit card information when participating in an educational program where a live client project involves accepting credit card transactions as payment from patrons. When students are acting in this capacity they must either a) comply with the provisions of this Section or b) be continuously observed while processing credit card information by an employee authorized to process credit card information under this Section.

## II. PROCEDURES

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

   a. Access to credit card information is restricted and controlled as described in Section I of this Policy.
   b. System and desktop passwords must be regularly changed when credit card information is processed on a particular system or desktop.
   c. Accounts shall be terminated or disabled immediately or as soon as reasonably possible for employees who leave employment with the College.

    d. Credit card information should not be stored in any format. This does not prohibit a third-party processor taking payments on behalf of the College from storing credit card information in conformity with the third-party processor's policies and procedures.

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

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

4. The College's Technology Department shall maintain additional procedures to ensure compliance with PCI DSS including but not limited to:

    a. Configuration of card processing procedures, including segmentation of local area networks and protection through deployment of firewalls,
    b. Logging control procedures,
    c. Wireless use procedures, and
    d. Encryption procedures.

---

**REFERENCES**

| | |
|---|---|
| **Statutory References** | None |
| **Regulatory References** | None |
| **Relevant Guidance** | "N.C. Community College Written Memoranda CC10-029" (2003) |
| **Policy Manual Cross-References** | None |

**POLICY HISTORY**

| | |
|---|---|
| **November 12, 2025** | Adopted. |