Title: Payment Card Security

Related Policy and Procedures:

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

I. DEFINITIONS

To ensure compliance with industry standards, the following definitions apply to this policy:

A. **Cardholder Data (CHD):** At a minimum, cardholder data consists of the full Primary Account Number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
B. **Cardholder Data Environment (CDE):** The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
C. **Sensitive Authentication Data (SAD):** Security-related information used to authenticate cardholders and/or authorize payment card transactions. This includes, but is not limited to, card verification codes (CAV2, CVC2, CVV2, CID), full magnetic stripe data, PINs, and PIN blocks.
D. **PCI DSS (Payment Card Industry Data Security Standard):** A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.
E. **Merchant Department:** Any College department or unit that has been approved by the Business Office to accept payments via credit or debit cards.
F. **Primary Account Number (PAN):** The unique payment card number (typically 14 to 16 digits) that identifies the issuer and the particular cardholder account.

II. PURPOSE AND SCOPE

The College is committed to protecting cardholder data (CHD) and maintaining the integrity of the Cardholder Data Environment (CDE). This policy applies to all employees, contractors, and third-party service providers who process, transmit, or store payment card information on behalf of the College.

III. DATA SECURITY STANDARDS

The College shall adhere to the Payment Card Industry Data Security Standard (PCI DSS) v4.0.

A. **Prohibited Storage:** Under no circumstances shall the College store **Sensitive Authentication Data (SAD)** after a transaction has been authorized.

B. **Encrypted Transmission:** All cardholder data transmitted over public or internal networks must be encrypted using industry-validated cryptography.
C. **Device Restriction:** Official College payment transactions must only be processed on college-approved hardware. The use of personal devices for capturing or processing cardholder data is strictly prohibited.

IV. IV. ADMINISTRATIVE OVERSIGHT

A. PCI Compliance Officer: The Chief Financial Officer (CFO), shall serve as the PCI Compliance Officer.
B. Annual Assessment: The College shall complete the appropriate PCI DSS Self-Assessment Questionnaire (SAQ) and Attestation of Compliance (AOC) annually.
C. IT Technical Responsibility: The Information Technology Department is responsible for the technical security and maintenance of the Cardholder Data Environment (CDE). This includes:

1. **Network Segmentation:** Maintaining firewalls and VLANs to isolate the CDE from the general College and guest networks.
2. **Access Control:** Implementing technical controls to restrict CDE access to authorized personnel only.
3. **Encryption and Patching:** Ensuring all data in transit is encrypted using industry-validated protocols and that all systems within the CDE are regularly patched and monitored for vulnerabilities.
4. **Hardware Integrity:** Collaborating with the Business Office to perform periodic inspections of point-of-sale (POS) terminals for evidence of tampering or skimming.

V. INCIDENT RESPONSE

In the event of a suspected or confirmed security breach involving cardholder data, the IT Department shall immediately execute the Cybersecurity Incident Response Plan. All affected systems shall be isolated to contain the breach, and data shall be preserved for forensic investigation by state authorities or a PCI Forensic Investigator (PFI) as required by N.C.G.S. § 143B-1320**.Legal Reference:** PCI DSS v4.0; N.C.G.S. § 143B-1320; N.C. Community College Written Memoranda CC10-029**.**

June 13, 2023	June 9, 2026	June 9, 2026
Date Approved by Board of Trustees	**Date of Last Review**	**Date of Last Revision**