PCI DSS COMPLIANCE POLICY

Related Board of Trustees Policy: BP
Approval: December, 2013
Revision:
NC Statewide Technology Standards (ed. August, 2010 Corrections):

PCI DSS Compliance Policy

Purpose: The Payment Card Industry Data Security Standards (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for the for the development, management, education, and awareness of the PCI Security Standards, while compliance with the PCI DSS is enforced by the individual card system brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Entities Affected by this Policy: All departments that collect, maintain or have access to credit card information must comply with this PCI DSS Compliance Policy. These currently include:

- Student Account Offices (New Bern and Havelock) accept and process credit cards for payment of tuition and fees, transcripts, parking fines, etc.
- Foundation - Accepts and processes credit card donations, special events, and fund raising.
- Public Radio East (PRE) – Accept and processes credit card donations, special events and fundraising.

Third party vendors that process, transmit or store credit card information for Craven Community College must be PCI compliant and approved by the Executive Director of Financial Services and Purchasing and the Dean of Technology & Facilities. Purchasing procedures as outlined on the college's website must be followed prior to engaging a third-party vendor. The current third party vendors approved by Directors are:

- ACI Worldwide, Inc./Official Payments and Nelnet – Student Accounts
- Blackbaud - Foundation
- Sun Trust/Intellipay– PRE

Third party vendors covered by this policy will be required to conduct their own PCI DSS assessment, and must provide sufficient evidence to Craven Community College to verify that the scope of the service providers' PCI DSS assessment covered the services provided to Craven Community College and that the relevant PCI DSS requirements were examined and determined to be in place. Annually, the college will verify third-party vendor compliance by checking the PCI Security Standards website.

Requirements:

Craven Community College requires compliance with all applicable PCI DSS requirements.

A Credit Card Security Incident Response Plan will be observed and implemented by an Incident Response Team.

Appropriate training will be provided to staff with security breach response responsibilities.

Enforcement:

The Executive Director of Financial Services and Purchasing and the Dean of Technology & Facilities and the Appropriate Department Head will investigate any reported violations of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy.

Revised: March 31, 2016

Return to Table of Contents