

Payment Card Processing Compliance

Version 2

 Print

Policy	REG07.85.01
Title	Payment Card Processing Compliance
Category	Finance, Operations and Auxiliary Services
Sub-category	eCommerce
Authority	Chancellor
History	Placed in University Policy Manual after EXPEDITED REVIEW, transitioned without substantive change from prior version, March 25, 2013; updated July 16, 2013; updated May 2016.
Contact	eCommerce Manager, 737-1133, ecommerce@ecu.edu
Related Policies	<p>University Student and Employee Computer Use Policy (https://policy.ecu.edu/08/05/04)</p> <p>PCI Security Standards Council (https://www.pcisecuritystandards.org/)</p> <p>North Carolina Office of the State Controller PCI Security Compliance Program (https://www.osc.nc.gov/state-agency-resources/payment-card-industry-pci-security-compliance-program)</p> <p>Network Use Regulation (https://policy.ecu.edu/08/10/03)</p>
Additional References	<p>ECU Merchant Card Processing (pdf) (https://financialservices.ecu.edu/wp-content/uploads/sites/86/2018/05/Merchant-Card-Processing.pdf)</p> <p>ECU Payment Card Industry (PCI) website (https://financialservices.ecu.edu/pci/)</p> <p>ECU PCI SharePoint Site</p>

1. Purpose

The purpose of this regulation is to ensure the security of all payment card holder data at East Carolina University.

2. Introduction and Background

The Payment Card Industry Security Standards Council, founded by all of the major credit card companies, has created a set of standards formally known as the Payment Card Industry Data Security Standard (PCI DSS). The intention of the PCI DSS is to help merchants ensure the security of payment card data by improving overall business practices thus reducing the likelihood of a security breach. The PCI DSS contains requirements

necessary for the secure collection, transmission, processing and storage of payment card data. All credit card merchants must incorporate the PCI DSS into their business practices in order to retain credit card processing privileges with their respective credit card companies.

The North Carolina Office of the State Controller (OSC) is charged with ensuring that all state agencies adopt and comply with the PCI DSS. East Carolina University, its campus payment card merchants and their agents must adopt and comply with the PCI DSS in order to retain credit card processing privileges as members of the Master Services Agreement that is provided by the OSC.

3. Responsible Officers and Parties

3.1 The Vice Chancellor of Administration and Finance is responsible for ensuring that all ECU payment card activity is PCI DSS compliant. The PCI Compliance Committee, as a delegate for the Vice Chancellor of Administration and Finance, is responsible for creating policies and procedures, administering and monitoring payment card activity to ensure compliance with the PCI DSS.

3.2 The PCI Compliance Committee's duties include, but are not limited to, the following:

3.2.1 Review New Payment Card Merchant Requests

3.2.2 Review Pending/Requested Changes to Existing Payment Card Systems

3.2.3 Approval/Denial Recommendations to ECU Financial Services

3.2.4 Administer and Review Self-Assessment Questionnaires Annually

3.2.5 University Education and Training on PCI DSS

4. Requirements within PCI Scope

All University departments, employees, agents, subcontractors, independent contractors and others with access to the cardholder data environment are required to adhere to the PCI DSS and University policies, regulations, standards, guidelines and procedures set forth and/or referenced in this regulation.

5. Violation Consequences

5.1 East Carolina University is responsible for the loss or theft of payment card account information and non-compliance issues because all campus payment card merchants are operating under a chain merchant identification number belonging to the University. However, ultimate responsibility for losses, thefts or non-compliance and related fines and/or consequences lies with the merchant department in which a compromise or non-compliant incident occurs. Outlined below are examples of fines and consequences.

5.1.1 A suspected incident, breach or compromise involving payment card data or the cardholder data environment must be reported immediately either to the eCommerce Manager or the ITCS Help Desk. If the event meets specific criteria, the eCommerce Manager will notify the North Carolina Office of the State Controller. A merchant failing to report immediately such events risks a penalty of \$100,000 per incident per Cardholder Information Security Program (CISP).

5.1.2 A merchant is subject to fines of up to \$500,000 per incident per CISP if it is non-compliant at the time of a data compromise.

5.1.3 Merchant department payment card processing privileges may be suspended or revoked as a result of the loss or theft of payment card data or for non-compliance with the PCI DSS.

5.1.4 Merchant department employees may be subject to disciplinary action as a result of a deliberate violation or negligence of the PCI DSS.

East Carolina University

E 5th Street | Greenville, NC 27858 (<https://www.google.com/maps/place/East+Carolina+University>) | 252-328-6131 (tel:+12523286131)
©2025 | [Terms of Use \(https://www.ecu.edu/terms\)](https://www.ecu.edu/terms) | [Accessibility \(https://accessibility.ecu.edu/\)](https://accessibility.ecu.edu/) | [Report a Barrier \(https://accessibility.ecu.edu/report-an-accessibility-barrier/?referrer=https%3A%2F%2Fpolicydev.ecu.edu%2Farchive%2F07%2F85%2F01%2F2\)](https://accessibility.ecu.edu/report-an-accessibility-barrier/?referrer=https%3A%2F%2Fpolicydev.ecu.edu%2Farchive%2F07%2F85%2F01%2F2)