WINSTON-SALEM STATE UNIVERSITY

PAYMENT CARD INDUSTRY COMPLIANCE POLICY

Policy

Winston-Salem State University (WSSU) is committed to safeguarding personal and account information conveyed in processing payment cards directly or through a third party. WSSU will comply with the Payment Card Industry Data Security Standards (PCI DSS) and E-Commerce policies of the Office of State Controller (NC OSC) Statewide Electronic Commerce Program, as they may be amended from time to time.

Scope of the Policy

This policy applies to all WSSU faculty, staff, students, temporary employees and any other persons who collect, process, transmit or store credit card information physically or electronically. Any other entity or individual using WSSU servers or the WSSU network must also abide by this policy. Hereinafter, all applicable persons will be referred to as "Department" for the purposes of this policy.

PCI Compliance

WSSU engages in a variety of activities that involve the collection of payments by credit card. The Payment Card Industry Security Standards Council publishes PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS that are required as part of the University's contract with its merchant card processor (https://www.pcisecuritystandards.org/index.php).

As a state agency, the University is also required to follow the E-Commerce policies published by the NC Office of State Controller as part of their Statewide Electronic Commerce Program. The PCI requirements apply to all systems that store, process, or transmit cardholder data. The WSSU environment does not include storage of cardholder data on any computer system or terminal. Credit card merchant accounts must be compliant with all applicable DSS for their method of payment acceptance. Maintaining PCI compliance is a continual process as each payment card brand has defined its own specific requirements for compliance, validation and enforcement.

All WSSU departments accepting payment cards must comply with the security requirements involved with being a payment card merchant. All WSSU departments that process payment card transactions also must comply with WSSU's defined methodologies and acceptable technology. Complete cardholder data may not be transmitted, processed, or stored on any University-owned or University-controlled devices, including its networks.

The Student Accounts and Cashiering Office (SACO) oversees WSSU's method for accepting and processing payment card transactions as well as distribution of policies, procedures, and other guidance required under PCI DSS and ongoing maintenance of a the PCI DSS compliance program. All departments wishing to process payment card transactions must contact the SACO for approval. Upon approval, SACO will establish a specialized Merchant Account Number for the department. The department then becomes responsible for achieving and maintaining compliance with PCI DSS, this policy, and SACO procedural requirements. Departments should contact SACO for a copy of the SACO procedures for PCI DSS compliance.

WSSU departments may not process credit cards under any circumstances without the required SACO approval and may not set up their own banking relationships for payment card processing.

Card Transaction Fees

Transaction fees may be charged to cover the cost of permitting a person to complete a transaction using a web application or other means of electronic access. The fee imposed must be approved by the SACO and General Administration. The transaction fees that are charged must be for conducting an electronic transaction, not for the use of a merchant card. Electronic access includes the internet and voice response systems but not mail orders, telephone orders, or a face-to-face transaction. The revenues from the transaction fee and expenditures funded by the fee must be accounted for separately to provide an audit trail on the collection and use of the fees. Expenditures may only be made for e-commerce initiatives and projects, to include any third-party related fees and merchant card processing services.

Annual Compliance Review

The Student Accounts & Cashiering Office in conjunction with Information Technologies is responsible for security breach management must review security breach procedures on an annual basis. The PCI DSS Incident Response Plan will be reviewed on an annual basis and will be modified and improved upon as industry security standards change. In addition, SACO will monitor PCI-DSS compliance for service providers on an annual basis. The review will include reconfirmation of certified PCI compliance of WSSU's third party vendors that accept payment card payments on behalf of the University.

Effective date: This policy becomes effective upon approval.
Adopted: This the 17th day of June 2016

____
Debra B. Miller, Chairman
WSSU Board of Trustees

____
Charles Wright, Secretary
WSSU Board of Trustees