Payment Card Merchant Security Policy

VSU Financial Services and Information Technology serve as leaders in the annual role of the University’s Payment Card Industry Data Security Standard (PCI DSS) compliance program.

VSU Financial Services coordinates payment card acceptance for all funds receipted on the University's ledgers. Payment card acceptance includes any approved, valid debit/credit card. VSU Financial Services acts as the liaison between campus merchant departments (who process payment card transactions for the sale of goods and/or services) and the University’s payment card processors. Methods for processing payment card transactions include point-of-sale card swipe terminals, internet credit card solutions, and various third-party software applications.

VSU Financial Services will consult with prospective and existing merchant departments, set up new campus merchants, and provide guidance, training and troubleshooting assistance related to payment card processing. The Division of Information Technology is responsible for campus Information Security and Acceptable Use policies (AUP), and will also provide guidance, may offer awareness training which includes best practice recommendations in protecting sensitive data, and will monitor adherence with the University’s Payment Card Merchant Security Policy. The AUP reads “All University supplied services and/or materials offered by the University will comply with credit card industry standards. No credit card data will be stored on or transverse the University computer network in an unsecured manner.” The Information Security policy mandates physical and logical security to systems and requires unique user names and passwords as well as a host of other requirements that proceed and/or compliment this policy.

Campus merchant departments must comply with Payment Card Industry Data Security Standards, must complete annual self-assessment questionnaires, and must attest to their PCI DSS compliance. Campus merchant departments shall be responsible for costs associated with PCI DSS compliance as well as any fines or other fees associated with their non-compliance. All Valdosta State University employees working with credit cards must read and agree to the conditions of this policy.

Approval from the Vice President for Finance and Administration is required before a campus merchant account for accepting credit cards can be established. Requesting departments must inform the Vice President for Finance and Administration of their need to become a campus merchant prior to engaging in any activity or purchasing a new system that will accept card payments. Those departments wishing to use credit card solutions must undergo a Credit Card Merchant Security Assessment conducted by the Division of Information Technology prior to the purchase of third party software or engaging in any contractual services. Departments not complying with approved safeguarding, storage, processing, transmitting and administrative procedures will lose the privilege to serve as a credit card merchant; individuals responsible may receive disciplinary action.
Any technology based equipment used in the processing of card and/or electronic payment transactions will be designated as an asset of VSU. Additionally, while a department may maintain local administrative rights to specific servers and processing equipment, an administrative account will be configured for central IT support.

Any VSU employee, contractor, consultant or agent who, in the course of doing business on behalf of the University, is involved in the acceptance of credit card data, handles cardholder data information, and/or is involved in the acceptance of card payments is subject to this policy.