

Augusta University

Policy Library

Credit Card Processing Policy

Policy Manager: Finance

POLICY STATEMENT

This policy applies to any department or individual accepting credit card funds on behalf of or in the name of Augusta University (AU).

This policy provides for centralized control of all credit card processing activities associated with the institution in order to facilitate compliance with the Payment Card Industry Data Security Standard (PCIDSS). Compliance with this standard ensures that our customers are protected against the risk of identity theft to the best ability of existing credit card processing technology. Compliance ensures Augusta University is not exposed to the risk of adverse publicity or fines associated with failure to protect customer bank and credit card information.

A breach of this type of data can result in fines, monthly penalties, infringement penalties, compensation costs, revenue loss and audits. The institution may be held responsible for all fraud losses incurred by the individual cardholders, the cost of reissuing the compromised cards, and additional costs associated with fraud prevention/detection activities required by the card associations. In addition, the University would experience increased card interchange rates, and elevation of merchant level requiring costlier Self-Assessment Questionnaire (SAQ) regulatory evaluations.

Locations accepting credit cards are responsible for ensuring that the equipment used to process credit card transactions are compliant with Payment Application Data Security Standards (PA-DSS). The credit card processor and software provider must be approved for use and provide the best value for the organization. Merchants must be responsible for awareness of the threats associated with credit card use, and take responsibility for this. Each location is responsible for ensuring all employees who process credit card transactions are properly trained. In addition, each location must complete an annual SAQ-Standard Self Assessment Questionnaire attesting to their compliance through the credit processor.

AFFECTED STAKEHOLDERS

Indicate all entities and persons within the Enterprise that are affected by this policy:

- Alumni Faculty Graduate Students Health Professional Students
 Staff Undergraduate Students Vendors/Contractors Visitors
 Other:

DEFINITIONS

PCI Data Security Standard: The Payment Card Industry (PCI) Data Security Standard details security requirements for merchants and service providers that store, process or transmit cardholder data.

Payment Card Application: Anything that stores, processes, or transmits card data electronically. In most cases, this does not include the hardware running the application unless the hardware and software

Office of Legal Affairs Use Only

Executive Sponsor: Vice President for Finance

Next Review: 10/2024

are intertwined similar to a credit card swipe terminal. This means that anything from a Point of Sale System to Website e-commerce shopping are all classified as payment applications. Therefore, any piece of software or hardware that has been designed to process credit card data is considered a payment application.

Payment card application infrastructure: Computing resources (i.e. servers, storage, network and storage switches, firewalls, physical racks containing these, and related software) which process, transmit, or store payment card data or can directly access such resources.

Credit Card Swipe Machine: Any device through which a credit card is manually swiped to read the credit card data embedded in the data strip on back of the card. Such devices may not be programmed to internally store credit card data. Devices internally storing credit card data are strictly prohibited by this policy and by the related Information Technology Standard referenced above. Also, devices that do not properly encrypt credit card data as it flows across on-campus servers are prohibited. Machines used for processing credit cards should be replaced by the department as new technology becomes available. When purchasing or replacing card machines, AU Information Security Risk and Compliance should be consulted regarding regulatory requirements as well as the Business Office to ensure the card machine is obtained through an approved channel and that it is compliant with the latest technology to ensure data security.

Credit Card Scanner: A device similar to a Credit Card Swipe Machine in which there is no data storage capability. Such devices serve only to electronically transmit data from the credit card magnetic strip to the software application processing such data. These devices must properly encrypt the data that is processed at the point of sale. When departments are purchasing or replacing equipment with this type of device, AU Information Security Risk and Compliance and the Business Office should be consulted to ensure the machine is obtained through an approved channel and that it is compliant with the latest technology to ensure data security.

OVERVIEW

Only PIN Transaction Security (PTS)-approved Credit Card processing machines with updated security standards such as point-to-point encryption (P2PE), approved devices that are listed on the PCI Security Standards Council website and only payment vendors who are approved as compliant via this website should be used.

Additionally, software, computers or networks used to transmit or store credit card data should be adequately secured with the involvement and input of the university's IT Department, to prevent unauthorized access to cardholder data due to improper equipment or security.

Credit card numbers should be secured. They should not be written down on paper, which encourages theft. If there are occasions where they must be written down, the information must be immediately shredded via a cross-cut shredder. Credit card data should never be stored for later use. If you have a special circumstance requiring review, you must present this to Information Security Risk and

Compliance immediately.

The University System of Georgia Board of Regents holds contracts with vendors offering merchant services, and payment gateway vendors. The merchant services vendor is typically affiliated with the current bank with which the University is affiliated. The payment gateway vendor must offer secure PCI and PA-DSS certified payment gateway over which to accept and transmit credit card data electronically to the processor. To facilitate compliance with PCI Data Security Standards for all credit card activities associated with Augusta University, the Institution strongly encourages all departments and operating units to utilize approved and licensed vendors to the greatest extent possible.

PROCESS & PROCEDURES

- Any individual or department accepting credit cards in the name of Augusta University or in association with Augusta University activities, services or contracts must contact the Bursar to register. The Bursar will provide a questionnaire upon inquiry to the Business Office. Registration information required to be provided includes:
 - The name and description of any credit card payment application currently used to transmit or store credit card data
 - Contact information for the software vendor
 - A brief description of the business process surrounding uses of the software
 - The make and model of any credit card swipe machines, scanners or smart terminals being used to store or transmit credit card data
 - Identification of all Augusta University workstations used to store or transmit credit card data
 - Name and contact information for any associated credit card processor, and the Augusta University merchant ID used by such processor
 - Justification for retaining the current credit card processor, should the department wish to seek a waiver for use of approved vendors.

Departments not currently using approved vendors for processing must convert unless a waiver is secured from the Controller's Division. In response to any request for waiver, the Bursar and Controller, in conjunction with an AU IT security administrator, will exercise all diligence to assess the adequacy of the current payment software and credit card data collection and processing mechanisms with respect to security concerns and PCI compliance. Departments and or individuals involved are expected to cooperate fully during this investigational process. A waiver will not be unreasonably withheld if the inquiring Department can document adequate levels of security and PCI compliance. The Controller's Office, in conjunction with IT personnel responsible for PCI compliance and overall data security administration, will issue a written determination letter.

- Requirements relating to the payment card application infrastructure are listed in the *Augusta University Information Security Standards for Payment Card Applications* and incorporated by reference herein. Considerations related to these requirements will contribute to whether

waiver is or is not granted for approved vendors exemption requests. These requirements include, but are not limited to the following:

- Servers that are part of the payment card application infrastructure and any workstations or systems that can otherwise directly access computing resources that contain payment cardholder data must be registered with AU IT Security as regulated computers
 - Workstations that are part of the payment card application must meet PCI Data Security Standards. AU Information Security reserves the right to determine the suitability of such workstations to support applications operating with the Augusta University payment card infrastructure.
 - Workstations and software must be strictly controlled for access on a “need to know” basis, and access rights continually monitored for any changes in roles or employment status of individuals.
 - Storage of credit card authentication data on workstations or other peripheral devices is strictly prohibited. Storage of any credit card information in written form or printed form is also prohibited. Scans are completed on a regular basis by AU IT to determine the location of such data. Storage of prohibited data may result in disciplinary action.
- New Payment Card Applications and associated Infrastructure must be coordinated through Augusta University IT Applications Support. Applications Support is responsible for coordinating communication and interaction between Augusta University, any application vendor(s), credit card processors, and other Augusta University groups in order to ensure secure implementation and operation. Applications Support will not implement systems other than approved vendors without first ensuring a waiver has been appropriately secured and documented.

REFERENCES & SUPPORTING DOCUMENTS

Augusta University Information Security Standards for Payment Card Applications, describing AU Information Technology standards and practices for managing a secure platform for Institution hosted payment card applications, specifically payment card transactions, and the data related to cardholders.

RELATED POLICIES

Intentionally left blank.

APPROVED BY:

Executive Vice President for Academic Affairs and Provost, Augusta University

Date: 10/11/2021

President, Augusta University

Date: 10/11/2021