Georgia College & State University

PCI-DSS Compliance Procedure

PCI Data Security Standard Compliance: Requirements for Offices Seeking to Outsource Payment Card Processing

Georgia College (GC) has a legal obligation to remain compliant with the Payment Card Industry (PCI) Data Security Standard (DSS). Under the PCI-DSS requirements, if GC outsources storage, processing, or transmission of cardholder data to a third-party service provider/merchant, the University's annual Report on Compliance (ROC) must document the role of each service provider or merchant that processes payment card transactions on behalf of the university. This documentation must clearly identify which PCI-DSS requirements are the responsibility of GC and which requirements are the responsibility of the service provider/merchant.

To reduce processing and compliance costs for the institution, all credit card readers will connect through a secure point-to-point dial-up connection. Credit card information will be used only at the time of the transaction and will not be stored on GC systems past that time.

In order to meet the PCI-DSS reporting requirements, GC requires each service provider/merchant who stores, processes or transmits cardholder data on behalf of GC to submit evidence of their PCI-DSS compliance on an annual basis. PCI-DSS compliance information will be collected, documented and reported annually through GC Information Technology.

There are two options for third-party service providers/merchants to validate their compliance with PCI-DSS:

1) They can undergo a PCI-DSS assessment on their own and provide evidence to GC to demonstrate their compliance. Refer to the PCI-DSS Self-Assessment Questionnaire Instruction Guide.

   or

2) Their services are reviewed during the course of their customers' PCI-DSS assessments. Refer to the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures found in the PCI Data Security Standard.   Notice: Georgia College does not extend PCI-DSS assessment services to third-party service providers/merchants.

Those vendors who are eligible to complete a PCI-DSS self-assessment questionnaire may submit their most recent Attestation of Compliance. Those vendors that are required to be PCI-DSS certified by a Qualified Security Assessor must submit their most recent certification. In either case, the evidence must be dated within the last 12 months.

Offices at GC desiring an agreement with a third party service provider/merchant to store, process or transmit cardholder data must:

- Document the business need for accepting credit card transactions.
- Meet with the Office of the Controller for justification and approval.
- Obtain the required PCI-DSS evidence and submit it to GC Information Technology (IT) and to the Vice President of Business and Finance for file.

Offices with ongoing agreements must obtain and submit the evidence of PCI- DSS compliance on an annual basis to Information Technology as it must be included in the University's annual Report on Compliance. It shall be the office's responsibility to resolve any missing service provider/merchant compliance documentation. An attestation of scan compliance only addresses section 11.2 of the PCI-DSS and will not be accepted as evidence of full service provider/merchant PCI-DSS compliance.

Reference

PCI-DSS Self-Assessment Questionnaire Instruction Guide:

https://www.pcisecuritystandards.org/documents/pci_dss_saq_instr_guide_v2.0.pdf

PCI Data Security Standard:

https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf