Credit Card Processing Policy

Volume: Finance & Administration
Responsible Office: Controller
Originally issued: March 2009
Revised: December, 2011

Policy Statement

This policy applies to any department or individual accepting credit card funds on behalf of or in the name of GHSU. This policy applies continuously.
No major conditions or restrictions apply

Reason for Policy

This policy provides for centralized control of all credit card processing activities associated with GHSU in order to facilitate compliance with the Payment Cardholder Industry Data Security Standard (PCI-DSS). Compliance with the Standard ensures that our customers are not unnecessarily exposed to the risk of identity theft in connection with their credit card transactions with GHSU, and that GHSU is not unnecessarily exposed to the risk of adverse publicity associated with failure to protect customer bank and credit card information or fines associated with non-compliance.

If the university were exposed to a breach of this type of data, fines up to $500,000 may be imposed by the card brands compromised. 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 more costly 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), and that the credit card processor that they use is approved for use and provides the best value for the organization. Locations must be evaluated for proper use and proper equipment, as well as utilize the processor that provides the best value for these types of transactions. Merchants must be responsible for awareness of the threats associated with credit card use, and take responsibility for this.

Entities Affected By This Policy

Any department or individual accepting credit card funds in the name of or in association with any GHSU activity or grant/contract on or off this campus must comply with this policy.

Who Should Read This Policy

Any department or individual on campus who accepts funds in the name of GHSU for any reason should read this policy.

Any and all personnel who have access to information resources (payment card applications and associated infrastructure, as defined below) that transmit, process, or store payment card data from students or any other GHSU customers are responsible for the application of this and related policies.

Informational Technology personnel responsible for security and for PCI compliance should also be familiar with this policy.

Contacts

Contact	Phone	e-mail/URL
Campus Business Office	706-721-2926	BUSINESS_OFFICE@georgiahealth.edu
Controller's Division	706-721-4116	jjones@georgiahealth.edu
Information Technology Security	706-721-1577	wray@georgiahealth.edu

Related Documents

GHSU Information Security Standards for Payment Card Applications, describing 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 card holders.

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 are intertwined similar to a credit card swipe terminal. This means that anything from a Point of Sale System to a Website e-commerce shopping are all classified as payment applications. Therefore any piece of software that has been designed to touch 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 device may or may not 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.

Credit Card Scanner: A device similar to a Credit Card Swipe Machine in which there is no data storage capability. Such device serves only to electronically transmit data off of a 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.

Overview

Credit Card Swipe Machines, especially older models, internally store consumer credit card data. Theft of such a device can result in theft of a cardholder's credit card data, which will invoke possible fines from the payment card industry.

Additionally, software, computers or networks used to transmit or store credit card data should be adequately secured, to prevent unauthorized access to card holder data.

Credit card numbers should be guarded. They should not be written down on paper, which encourages theft. If there are occasions where they must be written down, this occasion must be divulged prior to the occurrence to the Bursar and/or the Information Security Officer for evaluation. If no other form of data entry can be secured, the credit card data must only be on paper temporarily, and it must be stored in a secure location while not in use.

The University System of Georgia Board of Regents holds contracts with both First Data Merchant Services, the credit card processor GHSU currently utilizes to process the great majority of its credit card business, as well as with TouchNet Payment Gateway, a software vendor that offers a secured, PCI certified payment gateway over which to accept and transmit credit card data electronically to First Data Merchant Services. To facilitate compliance with PCI Data Security Standards for all credit card activities associated with GHSU, the Institution strongly encourages all departments and operating units to utilize TouchNet and First Data Merchant Services to the greatest extent possible.

Process/Procedures

- Any individual or department accepting credit cards in the name of GHSU or in association with GHSU activities, services or contracts must

contact the Bursar to register. Registration information required to be provided includes:

o The name and description of any credit card payment application currently used to transmit or store credit card data
o Contact information for the software vendor
o A brief description of the business process surrounding use of the software
o The make and model of any credit card swipe machines, scanners or smart terminals being used to store or transmit credit card data
o Identification of all GHSU work stations used to store or transmit credit card data
o Name and contact information for any associated credit card processor, and the GHSU merchant ID used by such processor
o Justification for retaining the current credit card processor, should the department wish to seek a waiver for use of TouchNet Payment Gateway and First Data processing.

- Departments not currently using TouchNet and First Data Merchant Services 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 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, will issue a written determination letter.
- Requirements relating to the payment card application infrastructure are listed in the GHSU 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 TouchNet/First Data exemption requests. These requirements include, but are not limited to the following:

  o 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 IT Security as regulated computers
  o All workstations must meet PCI Data Security Standards. GHSU IT Security reserves the right to determine the suitability of such workstations to support applications operating with the GHSU payment card infrastructure.
  o 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.
  o Storage of credit card authentication data on workstations or other peripheral devices is strictly prohibited. Scans are completed on a regular basis by IT to determine the location of such data. Storage of prohibited data may result in disciplinary action.

- New Payment Card Applications and associated Infrastructure, to include but not limited to TouchNet/First Data conversions, must be coordinated through GHSU IT Applications Support. Applications Support is responsible for coordinating communication and interaction between GHSU, any application vendor(s), credit card processors, and other GHSU groups in order to ensure secure implementation and operation. Applications Support will not implement systems other than TouchNet/First Data without first ensuring a waiver has been appropriately secured and documented.

Responsibilities

The responsibilities each party has in connection with the *Credit Card Processing Policy* are:

Departmental Director/Manager	Ensure that any credit card activities of which they are aware are disclosed to the Controller's Division (Campus Business Office/Bursar).
Controller's Division and IT	It is the joint responsibility of the Controller's Division (Bursar and Controller) and Information Technology (Information Security Officer) to make a reasonable and fair determination based on departmental needs and PCI / data security requirements as to any exemptions granted. If an exemption is granted, it shall only apply to the system at the time of assessment. If the system changes or upgrades are applied the system should be re-evaluated. (It is the responsibility of the departmental director to notify the Controller's Division and Information Technology Division of these changes.)
All Departments	Cooperate fully and on a timely basis with respect to any system modifications that may be required

	under this policy, and to bear the associated costs, if any.

Forms

None.

This entry was posted in *Controller's Division*, *Finance* and tagged *credit card processing*, *Payment Cardholder Industry Data Security Standard*. Bookmark the *permalink*. Both comments and trackbacks are currently closed.

« *Campus Invoicing & Collections Policy* *Departmental Deposits Policy* »