CREDIT CARD PROCESSING

POLICY AND PROCEDURES

Note: For purposes of this document, debit cards are treated the same as credit cards. Any reference to credit cards includes credit and debit card transactions.

Contents

Policy Statement

A. The approval process for all credit card processing activities will be as follows:

- The Director of Revenue, Receivable and Cashiering Services, Comptroller, Chief Information Security Officer (CISO) or delegate(s) must approve all credit card processing activities at Georgia State University before a unit enters into any contracts or purchases software and/or equipment. Please refer to the Georgia State University Credit Card Processing Procedures for additional information. This requirement applies regardless of the transaction method used (e.g., e-commerce, POS device, or e-commerce outsourced to a third party). Approved units must register their credit card processing information with the Office of Revenue, Receivable & Cashiering Services (RRCS).

- All technology implementation (including approval of authorized payment gateways) associated with the credit card processing must be in accordance with the *Georgia State University Credit Card Processing Procedures*, Payment Card Industry Data Security Standards (PCI-DSS), https://www.pcisecuritystandards.org, and the University System of Georgia Board of Regents policies. In addition, the implementation must be approved by the Director of Revenue, Receivable and Cashiering Services, Comptroller, Chief Information Security Officer (CISO) or delegate(s).

- Sensitive cardholder data should not be stored in any fashion on Georgia State University computers or networks. Transmission of sensitive cardholder data must follow guidelines for point of sale and e-commerce as described in the University credit card procedures. Credit card point of sale receipts should follow approved procedures for storage and retention. Exemptions to this must be approved by the Director of Revenue, Receivable and Cashiering Services, Comptroller, Chief Information Security Officer (CISO) or delegate(s).

Units approved for credit card processing activities must maintain the following standards:

- All employees (business managers, operations personnel, and technical staff) involved in e-commerce or POS transactions must attend annual PCI and University training.

- All units should create, maintain and test annually, business continuity and disaster recovery plans. A copy of the Compromise Incident Response Procedures can be found in the *Credit Card Processing Procedures*.

- All servers and POS devices will be administered in accordance with the requirements of the *Credit Card Processing Procedures.*

- All cardholder data should be treated the same as cash. It should be in a restricted, locked and fire secure area. Access to credit card processing systems and related information (i.e. forms) must be restricted to appropriate personnel. These individuals are defined as needing access to credit card information in order to perform their day to day job responsibilities. Destroy all media containing unnecessarily stored cardholder data. Cross cut shredding is the minimum requirement by which card holder data on paper is acceptably assumed destroyed. Shredding should be done as soon as it is no longer required for business purposes.

B. The university will utilize the CISO's appointed Certified PCI-DSS Internal Security Assessor and contract with an approved certified PCI 3rd party assessor to review our processes and determine any vulnerability as it relates to PCI compliance. Each unit responsible for credit card processing must have a completed PCI questionnaire on file with the CISO. This questionnaire needs to be reviewed annually to ensure compliance with this policy and the associated procedures. Each unit, with the exception of point of sale campus merchants, must also enroll and participate in network scans with the University CISO. Each campus merchant's questionnaire and scans will be documented and tracked by the approved third party assessor. The Office of Revenue, Receivable & Cashiering Services (RRCS), University Auditing and Advisory Services and the Office of Information Security will have access to each campus merchant's status on a continual basis. The CISO or delegate will, at the request of the unit, assist in the initial PCI questionnaire. Audits will be performed periodically by University Auditing and Advisory Services to confirm the results of the PCI questionnaire.

C. On an annual basis, the CISO and/or RRCS will provide appropriate training to all employees associated with credit card processing.

D. Campus merchants will report any anticipated changes in their credit card processing procedures using the Enterprise Change Management Process - http://technology.gsu.edu/help-center/#request.

E. Campus merchants and employees in key roles (as defined in this policy) must be aware and adhere to the University's policy and procedures.

F. Require a background check as a condition of employment to any employee hired to be involved with credit card processing including (but not limited to) key roles, such as cashiers, before hiring. Please refer to Section 103 of Classified Employee Handbook for the University's policy regarding background and credit checks.

G. Should you become aware cardholder data has been compromised, you must follow the Compromise Incident Response Procedures as outlined in the *Credit Card Processing Procedures*.

Revisions and Exceptions:

This policy should be reviewed at least annually and revised as needed according to new standards and laws. This policy may be revised only with approval of the Comptroller and CISO of Georgia State

University. The Comptroller and the CISO may grant exceptions to this policy or revise the *Credit Card Processing Procedures* document provided the revisions or exceptions meet PCI-DSS guidelines.

Failure to comply with this policy and the associated required procedures will be deemed a violation of University policy and subject to disciplinary action up to and including termination as noted in the Employee Handbook Conduct Guidelines. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services.

The following offices and individuals shall be notified in writing with any subsequent revisions or amendments made to this policy:

- Comptroller
- Chief Information Security Officer
- Director of Revenue, Receivable and Cashiering Services

Reason for Policy

This policy provides requirements and guidance for all credit and debit card processing activities for Georgia State University.

At the initial publication of this policy, the following sources were consulted and provided the basis for this program: ISO 17799, Payment Card Industry (PCI) Security Standards, and the Card Association Merchant Operating Regulations (Visa, MasterCard, American Express, and Discover). As card association regulations change, this policy will be updated as needed, and adhered to on a continued basis.

This policy deals with access to Georgia State University's computing and network resources. All relevant provisions in the Information Security Policy and Ethics Policy are applicable and included by reference in this document.

- https://app.gsu.edu/policies/policy_index.cfm?view_policy=4608 (University Information Systems Use)
- https://www.pcisecuritystandards.org (Payment Card Industry Security Standards)
- http://www.usg.edu/information_technology_handbook/section5/C2256 (Minimum Security Standards for USG Networked Devices
- http://www.usg.edu/information_technology_handbook/print/section5 (Information Security)
- https://app.gsu.edu/policies/policy_index.cfm?view_policy=4462 (USG Password Security and Composition Standard)

Procedures

The *Credit Card Processing Procedures* carries the full force of this policy. This separation allows for easier modifications to the procedures due to the changing nature of business, technology and security.

Georgia State University currently accepts four major credit cards (American Express, Discover, MasterCard and Visa) for payment of services rendered and goods sold. Debit cards with the Discover, MasterCard, and Visa logos are also accepted. Other cards accepted via e-commerce using the Discover Network Partnership are China Union Pay, Diners Club, JCB, and PayPal. All campus merchants are required to process card transactions through the merchant services provider selected by the University.

General guidelines

1) Any University unit wishing to accept credit cards for goods and/or services should complete a Credit Card Merchant Application. Applications will be reviewed to ensure your request for processing credit card sales is in compliance with current University policies.

2) If specialized software and/or systems are required, the Office of Revenue, Receivable & Cashiering Services, Information Security Officer, Information Technology Auditor, and the applicable computer support unit will work with the campus merchant to ensure processing standards and safeguarding measures are met.

3) All campus merchants accepting credit cards for payment must comply with the Georgia State University Credit Card Processing Policy, Payment Card Industry (PCI) Standards, Board of Regents policy, Gramm-Leach-Bliley Act (GLBA) and the FTC Safeguards Rule: GSU Information Security Plan to protect the private financial information of University customers. The GLBA and FTC Safeguards Rule are available at https://app.gsu.edu/policies/search_policies.cfm?view_policy=4201.

4) Access to cardholder information should be limited to only those persons whose job requires such access.

5) If any campus merchant should become aware that cardholder data has been compromised; you must follow the Compromise Incident Response Procedures as outlined in the *Credit Card Processing Procedures*.

6) A Payment Card Industry (PCI) Questionnaire will be dispersed annually to each campus merchant for review and update as needed.

7) Campus merchants and employees in key roles (as defined in this policy and procedures) must participate in all training sessions offered.

8) Campus merchants operating point of sale equipment/ software must adhere to the following standard/policy which states personal use is prohibited on any computer or electronic device used for credit card processing, and as such reasonable measures shall be taken to limit personal use or any other unintended use of computers and devices that store, process or transmit credit card data. These reasonable measures include, but are not limited to:

- Anti-virus software

- Firewalls

- Automatic updating of the operating system

No web browsing may be done on this computer or electronic device except for web sites related to credit card processing.

- https://www.pcisecuritystandards.org (Payment Card Industry Security Standards)
- http://www.usg.edu/information_technology_handbook/section5/C2256 (Minimum Security Standards for USG Networked Devices

9) All departments are required to have written procedures for receiving, processing and storage of credit card information.

Guidelines for Point-of-Sale Transactions

1) The Office of Revenue, Receivable & Cashiering Services will coordinate all credit cards processing for the University. The Director of Revenue, Receivable and Cashiering Services (RRCS), Comptroller, Chief Information Security Officer (CISO) or delegate(s) must approve all credit card processing activities at Georgia State University before a unit enters into any contracts or purchases software and/or equipment.

2) All card transactions will be processed on equipment compatible with the processing platform(s) of the University's card processor.

3) Effective July 1, 2004, all customer receipts must truncate the card number so only the last four digits are printed (http://www.legis.ga.gov/Legislation/en-US/display/20032004/HB/213).

4) Campus merchants requiring equipment for point-of-sale (POS) transactions must contact the Office of Revenue, Receivable & Cashiering Services before such equipment is purchased. The Office of Information Security and University Auditing and Advisory Services will be consulted prior to equipment purchase if the requested equipment is not standard.

An email request must be submitted to the Office of Revenue, Receivable & Cashiering Services (rrcs@gsu.edu) for assistance with vendor selection. Any vendor chosen by a campus merchant must be Payment Card Industry (PCI) compliant and remain certified as compliant by the card associations.

5) Campus merchants should maintain a listing of all devices used, location of them, model, serial number and the personnel that have access to the device(s). Periodically inspect device surfaces to detect tampering and substitution - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

6) On a daily basis, the campus merchants processing credit card payments via POS devices must balance transactions and settle their sales electronically to the merchant services provider.

7) The campus merchant will send an e-mail to Accounting Services no later than noon of the day following settlement with the pertinent information so the sales revenue can be recorded in the University accounting system. Campus merchants should send an email to treasury@gsu.edu using the *Credit Card Transmittal Form*. It is important that campus merchants reconcile their point-of-sale transactions when they are settled.

8) In order to reduce fraud, credit card companies recommend the following procedures for processing cards for:

Card Present Transactions (in-person)

- Ask for identification at the point of sale to verify the card holder is using the card
- Always swipe the card through the terminal/point of sale device, if applicable
- Obtain authorization for every card sale
- Ask the customer to sign the sales receipt
- Match the printed number on the card to the four digits of the account number displayed on the terminal
- Compare name and signature on the card to those on the transaction receipt
- If you believe the card number or sale is suspicious, make a Card Present - Code 10 Call to the voice authorization center for the card being used.

Code 10 calls

Code 10 calls allow GSU merchants to alert card issuers of suspicious activity and to take appropriate action when instructed to do so. You or your supervisor should make a Code 10 call to your voice authorization center whenever you are suspicious about a card, cardholder, or a transaction. The term "Code 10" is used so the call can be made at any time during a transaction without arousing a customer's suspicions.

Making a Code 10 during a transaction

- You or your supervisor will call the credit card company's voice authorization center, and say, "I have a Code 10 authorization request."
- It is important to note that Code 10 calls can be time consuming. The call may first be routed to a representative of your merchant bank that may need to ask you for some merchant or transaction details. You will then be transferred to the card issuer and connected to a special operator who will ask you a series of questions that can be answered with a simple yes or no.
- When connected to the special operator, answer all questions calmly and in a normal tone of voice. Your answers will be used to determine whether the card is valid.
- Follow all operator instructions.
- If the operator tells you to pick up the card, only do so if recovery is possible by reasonable and peaceful means. GSU employees are not obligated or expected to confiscate credit cards.

Making a Code 10 call after a transaction

- Sometimes you may not feel comfortable making a Code 10 call while the cardholder is at the point of sale or you may become suspicious of a cardholder who has already left the store even if the transaction was not completed.
- It is important to know that Code 10 calls can be made even after a cardholder leaves the store. A Code 10 alert at that time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.
- Be prepared to provide as much customer information as you can - e.g. name on card, type of card (e.g. MasterCard) and card number.

Card Not Present Transactions (phone or fax)

· The University approved *Credit Card Authorization Form* is strongly recommended for card not present transactions.

· Obtain cardholder name, billing address, shipping address (if different from billing address and if applicable), account number, and expiration date.

· Verify the customer's billing address either electronically (by entering the zip code in the POS device) or by calling the credit card automated phone system.

· Obtain a signature for goods or services where the recipient is not the card holder.

· Maintain credit card receipts and all delivery records for the retention period as specified in the Record Retention section of this document.

9) Campus units must not accept or send credit/debit card information via email.

What should you do if Cardholder Information is received via email?

If cardholder information is received via email, campus merchants should follow the following procedure:

- The email must be deleted immediately from both your "In Box" and "Trash" folders.
- The campus merchant should notify cardholder that transaction will not be processed. Do not use "reply". The campus merchant should send a new email so that the cardholder information is not included in the response, adding the following (or similar) text to your email:

  "*Georgia State University does not accept or process credit card information provided via email. That would be against Payment Card Industry Compliance Standards and University Policy. Therefore, your transaction will not be processed. Please contact us to request available payment options*."

10) All point-of-sale terminal transactions must be batched and transmitted to the card processor on a daily basis. Transmission of sensitive cardholder data should be encrypted using 128 bit encryption and purged after settlement.

11) Those units, which utilize a fax machine for credit card orders, must operate a stand-alone fax machine connected via Plain Old Telephone Service (POTS) Analog line only. Multipurpose machines will not be allowed for receiving any credit card information. The stand-alone fax machine must be located in a secure area away from public traffic.

12) Access to the physical location of credit cardholder data should be in a restricted, locked and fire secure area where only authorized persons are allowed. Any visitors in this restricted area should be identified and escorted at all times.

13) Cardholder data is not to be taken or distributed for unauthorized purposes.

Guidelines for E-Commerce Transactions

1) The Office of Revenue, Receivable & Cashiering Services will coordinate all e-commerce processing for the University. No individual department may enter into a contract with a card processor without approval of the Director of Revenue, Receivable and Cashiering Services (RRCS), Comptroller, Chief Information Security Officer (CISO) or delegate(s).

2) Departments should contact and seek approval from the Office of Revenue, Receivable & Cashiering Services prior to purchase of specialized software or equipment so that customized processing

applications are reviewed in conjunction with policy and procedure. The Office of Revenue, Receivable & Cashiering Services, the Office of Information Security, and the applicable computer support unit will work with the department to ensure processing standards and safeguarding measures are met.

3) All card transactions must be processed through a payment gateway approved by the Director of Revenue, Receivable and Cashiering Services (RRCS), Comptroller, Chief Information Security Officer (CISO) or delegate(s).

An email request must be submitted to the Office of Revenue, Receivable & Cashiering Services (rrcs@gsu.edu) for assistance with vendor selection. Any vendor chosen by a department must be Payment Card Industry (PCI) compliant and remain certified as compliant by the card associations.

4) To the extent possible, card processing transactions should be performed on the website of the payment gateway (i.e., the customer should enter sensitive cardholder data on a payment engine website) and not on University computer or network resources.

5) No campus merchant should store or process any sensitive cardholder data on any University computer or server. All sensitive cardholder data should be maintained by an approved service provider. All outside service providers must comply with the Payment Card Industry (PCI) standards.

6) All IP based point of sale devices and/or ecommerce transactions must be batched and transmitted to the card processor daily. For IP based point of sale devices, sensitive cardholder data must be encrypted using 128 bit encryption and purged after settlement. Transmissions for IP based point of sale devices should be coordinated and approved by the Chief Information Security Officer (CISO) or delegate.

7) It is strongly encouraged that campus merchants reconcile their e-commerce transactions on a monthly basis.

8) When the Office of Revenue, Receivable & Cashiering Services receives charge back inquiries from the credit card companies, the applicable campus merchant will be contacted to provide the necessary information about the sales transaction in question.

9) Cardholder data is not to be taken or distributed for unauthorized purposes.

10) The Chief Information Security Officer (CISO) will be responsible for scheduling quarterly scans.

Technical Specifications

Each University unit processing credit cards will be responsible for adhering to the credit card merchants' data security program. The Office of Information Security will maintain links to the various merchant's data security programs at http://technology.gsu.edu/technology-services/it-services/security/. Any questions with regard to the technical specifications should be directed to the Chief Information Security Officer (CISO).

Each campus merchant ID assigned will have at least one person subscribed to the University credit card listserv to receive updates on the credit card policy and procedures.

Compromise Incident Response Procedures

Should you become aware that any cardholder data was subject to compromise, you should follow the steps outlined below within 24 hours:

1) Alert the following immediately:

- Office of Information Security
- Office of Revenue, Receivable & Cashiering Services

Note: if the compromise includes physical devices (e.g. computer, POS, etc.), please contact the University Police as well.

2) Immediately work with the Office of Information Security to limit the exposure. Prevent the further loss of data by doing the following:

- Do not access or alter compromised systems
- Isolate compromised systems from the network
- Preserve logs and electronic evidence
- Log all actions taken
- Be on high alert and monitor all systems

3) The Office of Revenue, Receivable & Cashiering Services will assist the campus merchant in notifying the third party vendor, if applicable.

4) The Office of Revenue, Receivable & Cashiering Services will contact the campus merchant services provider, University Legal Affairs Office and University Auditing and Advisory Services at this time.

Forms/Instructions

Credit Card Authorization Form

Credit Card Merchant Application Form

Credit Card Transmittal Form

Marketplace Access Request Form

Additional Contacts

Office of Revenue, Receivable and Cashiering Services, 404-413-3251, rrcs@gsu.edu

Office of Accounting Services, 404-413-3070, treasury@gsu.edu

Office of Information Security, 404-413-4357

Office of University Auditing and Advisory Services, 404-413-1310

Responsibilities

Responsible University Senior Administrator: Senior Vice President for Finance & Administration

Responsible University Administrator: Comptroller/Associate Vice President for Finance & Administration

Policy Owner: Director of Revenue, Receivable & Cashiering Services

Policy Contact: rrcs@gsu.edu

Phone Number: 404-413-3251

Record Retention

Campus merchants should maintain adequate records of the sales transactions. Daily sales totals, receipts, logs, etc. substantiating revenue should be stored for 5 years in accordance with state record retention policies (Board of Regents, Records Retention Series M - (http://www.usg.edu/records_management/schedules/M). Other documents with cardholder data such as the *Credit Card Authorization Form* (without the bottom section) should be stored in a locked filing cabinet or safe and only need to be retained for at least 2 years. At the time of disposal, all documents containing sensitive cardholder data should be shredded using a cross-cut shredder. Individuals with access to cardholder information should be limited to only those persons whose job requires such access, such as resolving credit card reconciling issues and disputes.

Policy/Procedure Definitions

Account Number: The unique number identifying the cardholder's account which is used in financial transactions

Campus Merchant: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the four members of PCI SSC (American Express, Discover, MasterCard or Visa) as payment for goods and/or services.

Cardholder Data: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. This data can be on paper or electronic.

Cardholder Information Security Program (CISP): CISP defines a standard of due care for securing Visa cardholder data, wherever it is located. CISP compliance has been required of all entities storing, processing, or transmitting Visa cardholder data.

CISO: Chief Information Security Officer

Credit Card Processing: Act of storing, processing, or transmitting credit cardholder data.

Data Security Standard (DSS): Data security standards mandated by American Express.

E-Commerce Applications: Any internet enabled financial transaction application.

Employee: Any employee as defined by the GSU Human Resources Policies and Procedures.

Employee In Key Roles: Any employee with the following roles concerning credit card sales: manager overseeing credit card sales, accountant for credit card sales, technical support to credit card solutions and equipment, and any other staff member with access to physically stored credit card receipts.

ISO 17799: The International Standards Organization document defining computer security standards.

Payment Application Data Security Standard (PA-DSS): Set of recommended practices for software vendors to create secure payment applications to help their customers comply with PCI.

Payment Card Industry Data Security Standard (PCI-DSS): Set of requirements adopted by the Card Associations to protect and safe guard against cardholder data exposure and compromise. This standard is inclusive of the Visa CISP, MasterCard SDP, and American Express DSS.

POS Device: Point-of-sale (POS) computer or credit card terminals either running as a stand-alone system or connecting to a server at Georgia State University or remotely off site.

RRCS: Office of Revenue, Receivable and Cashiering Services

Sensitive Cardholder data: This is defined as the account number, expiration date, CVC2/CVV2 (a three-digit number imprinted on the signature panel of the card), any sensitive authentication data subsequent to authorization, PVV (PIN Verification Value) and data stored on track 1 and track 2 of the magnetic stripe of the card.

Site Data Protection Program (SDP): The formal data protection program mandated by MasterCard. The SDP Program provides acquiring members with the ability to deploy security compliance programs, ensuring that online merchants and member service providers are adequately protected against hacker intrusions and account data compromises.

Web Development: The design, development, implementation and management of the user interface of the e-Commerce application.

Related Information

https://app.gsu.edu/policies/search_policies.cfm?view_policy=4201

https://www.pcisecuritystandards.org/