Office of Revenue, Receivables, and Cashiering Services

CREDIT CARD PROCESSING 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.

Table of Contents

Statement

Pursuant to the University's Credit Card Processing Policy, 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.

This requirement applies regardless of the transaction method used (e.g., e-commerce, Point of Sale (POS) device, or e-commerce outsourced to a third party). **Departments interested in opening new credit card merchant accounts must submit an ITS Help Desk ticket to initiate the application process**. Departments with the approval from the CISO, Comptroller and Director of RRCS to process credit card payments are considered Authorized Merchants and will be referred to as campus merchants throughout these procedures.

All technology implementation (including approval of authorized payment gateways) associated with the credit card processing must be in accordance with both the *Georgia State University Credit Card Policy and Credit Card Processing Procedures*, Payment Card Industry Data Security Standards (PCI-DSS). 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).

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. Storage and retention of credit card point of sale receipts should follow approved procedures. Exemptions to this must be approved by the Director of Revenue, Receivable and Cashiering Services, Comptroller, Chief Information Security Officer (CISO) or delegate(s).

Scope

All individuals with responsibility, authority, and stewardship over payment card transactions on behalf of the University. All persons who handle payment card transactions assume the responsibility for following the procedures outlined below.

Reason for the Procedures

These procedures provide requirements and guidance for all credit and debit card processing activities. 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 continuous basis.

This policy also relates to access to the 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.

Overall Requirements

Departments accepting payment cards on behalf of the Georgia State University for goods or services must have the prior approval of the CISO and the Comptroller to process card holder data.

Departments must designate a full-time employee within that department who will have primary authority and responsibility for payment card and/or ecommerce transaction processing within that department. Any changes to the person filling this role should be reported to RRCS. This individual will be responsible for the department complying with the security measures established by the Payment Card Industry and University policies. In addition, they are responsible for ensuring that any employee or a contractor who handles payment card transactions takes the annual PCI training, signs the training acknowledgement, and, if applicable, undergoes the appropriate background and credit check before any access is granted. This employee is considered the campus merchant. Please note that students are only allowed to handle cardholder data (CHD) if they are employees of the University.

Departments may only use the services of vendors which have been approved by RRCS to process payment card transactions regardless of whether the transaction is point of sale (POS), mail or telephone order, or internet-based.

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

1. **Departmental Procedures**: Per the Payment Card Industry Security Standards Council (PCI SSC), each department that handles payment card information must have documented procedures that are consistent with the University policy and cover the processes for complying with the current version of the Payment Card Industry Data Security Standards (PCI DSS). Departmental procedures should be reviewed, signed and dated by the Department Manager or designee on an annual basis indicating compliance with the University's Credit Card Processing Policy. These procedures also must be submitted to and approved by their Dean or Vice President, the IT Security Officer, and the Comptroller's Office.

   Departmental procedures must thoroughly describe the entire transaction process and will include, but are not limited to, the following:
   - Segregation of duties
   - Deposits
   - Reconciliation procedures
   - Physical security
   - Information disposal
   - Data retention

- Cash register procedures (if applicable)
- Incident response

2. **Disaster Recovery and Business Continuity**: 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 on p. 15 of these procedures.

3. **Potential Data Compromise or Security Breach:** Units must follow the Compromise Incident Response Procedures as outlined below in the event cardholder data has been compromised

4. **Complete the Annual PCI Compliance Checklist:**
   a. Collect an Attestation of Compliance (AOC) from any service providers with whom cardholder data is shared, or that could affect the security of your customers' cardholder data.
   b. Review departmental procedures to ensure that they are current and accurate.
   c. Test disaster recovery and business continuity plans
   d. Complete the Self-Assessment Questionnaire (SAQ) that has been assigned by the CISO.
   e. Review and update the equipment inventory: Includes a list of devices and a list of who is explicitly authorized to use devices
   f. Attend annual GSU PCI Compliance training session (all business managers, operations personnel and technical staff involved in e-commerce or point of sale transactions)
   g. Complete annual acknowledgement of GSU PCI Compliance policies and procedures

5. **Data Security:** All cardholder data should be treated the same as cash. It should be in a restricted, locked and fire secure area. Cardholder data must not be sent or received via email. Campus merchants shall coordinate with the GSU Cyber Security Office (security@gsu.edu) for assurance of the encrypted transmission of cardholder data across open, public networks and at rest.

6. **Cybersecurity**: All servers and POS devices must be administered in accordance with the requirements of the Payment Card Industry – Data Security Standards. GSU Cyber Security Office is responsible for assurance of the data security standards. Campus merchants shall not adjust the security settings, download software, or alter network configuration without consultation with GSU Cyber Security (security@gsu.edu)

7. **Network Scanning:** Each unit, must be enrolled and participate in network scans with the University CISO or Cybersecurity unit.

8. **Restricted Access**: 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.

9. **Criminal Background and Credit Checks**: Units must require a criminal background and credit 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.

10. **Usage Limitations**: Campus merchants operating point of sale equipment/ software must ensure use of any computer or electronic device used for credit card processing is strictly limited to business purposes and take reasonable measures to limit personal use, or any other unintended use, of computers and devices that store, process or transmit credit card data.

11. **Record Retention and Destruction**: 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. Cardholder data must not be sent or received via email.

12. **Processing Procedures**: Campus merchants must follow the guidelines as outlined below unless departmental procedures have been reviewed and approved by RRCS. Procedures will be reviewed no less than annually. 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.

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 the University processes and determine any vulnerability as related to PCI compliance. 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. Audits will be performed periodically by the University Auditing and Advisory Services to confirm the results of the PCI questionnaire.

Revisions and Exceptions

This procedure should be reviewed at least annually and revised as needed according to new standards and laws. This procedure may be revised only with approval of the Comptroller and the CISO of Georgia State University. The Comptroller and the CISO may grant exceptions to this procedure provided the revisions or exceptions meet PCI-DSS guidelines.

Failure to comply with the policy and 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 the policy and procedures is subject to disconnection of network services.

Procedures

The *Credit Card Processing Procedures* carry the full force of the University's Credit Card Processing 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 credit card merchant services provider selected by the University.

General Guidelines: All transactions

1) Any University unit wishing to accept credit cards for goods and/or services should complete a PCI Application for new Payment Card Merchants (insert link). Cybersecurity team will review the application and put infrastructure in place. Campus merchants and their security operations team will be approved to place an order for the new terminal.
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 both the Georgia State University Credit Card Processing Policy and Procedures.
4) Campus merchants must ensure, in collaboration with the Office of Cybersecurity, that adequate hardware and software protections are installed and updated. These include, but are not limited to anti-virus software, firewalls, and automatic updating of the operating system.
5) No web browsing may be done on the computer or electronic device except for websites related to credit card processing.
    a. https://www.pcisecuritystandards.org (Payment Card Industry Security Standards)
    b. http://www.usg.edu/information_technology_handbook/section5.11 (Minimum Security Standards for USG Networked Devices)
6) All campus merchants are required to have written procedures for receiving, processing and storage of credit card information.

Guidelines for Point-of-Sale (POS) Transactions

1) RRCS will coordinate all credit cards processing for the University. The Director of 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, University Auditing and Advisory Services will need to be consulted prior to equipment purchase if the requested equipment is not standard.
5) 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.
6) The campus merchant will complete the *Cashiering Deposit Remittance Form* and submit it in hard copy along with the credit card terminal batch receipt to the Cashier's office so the sales revenue can be recorded in the University financial management system. It is important that campus merchants reconcile their point-of-sale transactions when they are settled.
7) All point-of-sale terminal transactions must be batched and transmitted to the card processor daily. Transmission of sensitive cardholder data should be encrypted using 128-bit encryption and purged after settlement.
8) In order to reduce fraud, credit card companies recommend the following procedures for processing cards:

Card Present Transactions (in-person)

Transactions are considered "card present" if the CVV1 is submitted at the time of the transaction. The CVV1 is **not** the three-digit verification code that is visible on the card and more commonly known; that is the CVV2 or CVC2. The CVV1 is stored on the magnetic stripe of a payment card or on the integrated chip of an EMV or NFC payment card. Clearly in order to then be a "card present" transaction, the physical card must be presented at the time of the payment and the payment data entered by swiping (magnetic stripe), inserting (EMV) or tapping (NFC) the card.

If your department accepts in-person payments, please include these guidelines in your departmental procedures.

A. Attach all form(s) where payment card information is requested (if applicable)

C. Review Card Security

i. Is the card valid? The card may not be used after the last day of the expiration month embossed on the card. Never accept an expired card.

ii. Only the actual card/account holder should be using the card.

iii. Does the customer's signature on the charge form (if applicable) match the signature on the back of the card? Compare the signatures and make sure that the signed name is not misspelled or otherwise obviously different.

iv. Does the signature panel on the card look normal? Check to be sure that it has not been taped over, mutilated, erased, or painted over. Obvious physical alterations to the card could indicate a compromised card.

v. Does the account number on the front of the card match the number on the back of the card and the receipt display? If the numbers do not match, or if they are covered or chipped away, this could indicate an altered card.

Suspicious Behavior

- Customer appears nervous or anxious or rushes you at closing time.
- Customer makes larger than normal dollar amount transaction.
- Customer takes the card back quickly from you preventing you from checking the security features.
- Customer makes numerous small purchases.
- Customer asks you to manually key a transaction providing the card number from memory, a slip of paper or an old sales voucher.
- Customer needs to see the card to sign the sales receipt.
- Multiple cards presented. Be wary of customers who give you more than two card numbers or try to split a transaction.
- Customer make purchases, leave the premises, and then return to make more purchases.

vi. Does the name on the customer receipt match the embossed name on the front of the card? If the name is different, this could indicate an altered card.

b. In-Person Manually Keyed Transactions Prohibited: Manually keying in the card account information carries a higher risk of fraud since many of the built-in card security features cannot be accessed. If the magnetic stripe on the back of the card is unreadable or the EMV is not working, do not manually key the account information. Return the card to the cardholder and do not process the transaction.

c. Report Suspected Card Fraud

i. If you suspect the card is fraudulent, contact your supervisor to determine if additional assistance is necessary.

ii. If the supervisor suspects fraudulent or suspicious activity, please contact the GSU Police Department and RRCS immediately.

B. Retain all credit card terminal receipts.

C. Place the credit card terminal receipts in a designated, safe location until the end of day batch and settlement processes have been run.
D. Oversight of the card reader (NOTE: *PCI DSS Requirement 9.9 requires that all card-reading devices must be checked, and those checks must be logged*)

   a. Log terminal information into the **Credit Card Terminal Inventory List** and conduct inspections of the terminal at the beginning of each work day to determine if it has been tampered with or exchanged (i.e. verify stickers have not been removed and re-affixed, skimmers attached at the swipe or EMV insert, pry marks at seams or EMV insert, same model, same serial number, etc.). Enter the results of your inspection on the Credit Card Terminal Inspection Log provided by Cyber Security.
   b. Report any tampering as a security breach per the Incident Response Procedures below. A copy of the current Incident Response Plan is provided to each campus merchant on an annual basis by IIT.
   c. Keep the machine in a locked area when not in use or after hours.

Individuals responsible for handling in-person payments should be designated by the campus merchant or designee and regularly updated. A list of these individuals must be maintained and available upon request.

Card Not Present Transactions

Transactions are considered "card not present" if the CVV1 is not submitted at the time of the transaction because the physical card is not presented. Payments made over the telephone or Internet or sent via mail fall into this category.

Remember, the liability for all card not present transactions rests with the campus merchant. The more information you gather to satisfy yourself that the transaction is valid the more chance you have of identifying fraud and reducing the chargeback risk.

A. The University approved *Credit Card Authorization Form* **(https://finance.gsu.edu/download/credit-card-authorization-form-pdf/?wpdmdl=2468&refresh=5dc5c8cac87a31573243082)** is required for card not present transactions.
B. Obtain cardholder name, billing address, shipping address (if different from billing address and if applicable), account number, and expiration date.
C. 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.
D. Obtain a signature for goods or services where the recipient is not the card holder.
E. Maintain credit card receipts, credit card authorization forms, and all delivery records for the retention period as specified in the Record Retention section of this document.

Mailed in Payments

If your department accepts payments via mail, please detail the departmental procedures below.

A. Departments must use the *Credit Card Authorization* form.
B. At least two people should be responsible for opening the mail and logging any payments onto a departmental payment log. If possible, these staff members should alternate days.
C. Bundle together all card payment forms and attach the departmental payment log.
D. Hand over the bundle to the person responsible for entering the payment(s).
E. Process the payments using the approved departmental method (i.e. hosted payment application, card reader, etc.) and print out two copies of the receipt.
F. The portion of the credit card authorization form containing the payment card information must be destroyed after the transaction has been processed in an approved PCI manner. Options for acceptable destruction include removing and cross-cut shredding or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Writing over the cardholder data (CHD) with a black marker is NOT acceptable.
G. Return a copy of the receipt to the customer via the approved departmental method which is {mail or in-person}.
H. If necessary, forward the payment confirmation to the event coordinator or person responsible for the class.
I. Place the credit card terminal merchant copy of the receipt in a secure location until the end of day batch process has been run.

Individuals responsible for opening and distributing the mail must be designated by the campus merchant or delegate. A list of these individuals must be maintained by each campus merchant and available upon request.

Telephone Payments

A. All telephone payments should be entered in the credit card terminal or application during the call if possible. Do not accept payment information via a voicemail/phone message.
B. If payment data must be written down, it should be logged on the Credit Card Authorization Form and processed immediately after the call has concluded. The portion of the form containing the payment card information must be destroyed after the transaction has been processed in an approved PCI manner. An option for acceptable destruction include removing and cross-cut shredding the form. Writing over the cardholder data (CHD) with a black marker is NOT acceptable.
C. If the department uses a payment application, each person taking telephone payments must have a unique login; **shared logins are explicitly forbidden in the PCI DSS.**

Individual(s) with responsibility for telephone payments must be designated by the campus merchant or delegate. A list of these individuals must be maintained by each campus merchant and be available upon request.

Email or Fax Payments

Departments must NOT accept or send credit/debit card information via email or fax.

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

If cardholder information is received via email, campus merchants should follow these procedures:

- 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. This action is against Payment Card Industry Compliance Standards and the University Policy. Therefore, your transaction will not be processed. Please contact us to request available payment options*."

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

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

- Options for acceptable destruction include removing and cross-cut shredding or rendering it unreadable on the form (i.e. hole-punch through the card number, expiration date, and security code). Writing over the CHD with a black marker is NOT acceptable.

Guidelines for E-Commerce Transactions

1) RRCS 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 RRCS, Comptroller, Chief Information Security Officer (CISO) or delegate(s).
2) Departments should contact and seek approval from RRCS prior to purchase of specialized software or equipment so that customized processing applications are reviewed in conjunction with University's policy and procedures. RRCS, 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 RRCS, Comptroller, Chief Information Security Officer (CISO) or delegate(s).

4) 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.
5) 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.
6) 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.
7) All IP based point of sale devices and/or ecommerce transactions must be batched and transmitted to the payment 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.
8) It is strongly encouraged that campus merchants reconcile their e-commerce transactions on a monthly basis.
9) When the Office of Revenue, Receivable & Cashiering Services receives charge back inquiries from the credit card merchant, the applicable campus merchant will be contacted to provide the necessary information about the sales transaction in question.
10) Cardholder data is not to be taken or distributed for unauthorized purposes.
11) The Chief Information Security Officer (CISO) will be responsible for scheduling quarterly scans.

Individual(s) with responsibility for online payments must be designated by the campus merchant or delegate. A list of these individuals must be maintained by each campus merchant and be available upon request.

End of Day Batch and Reconciliation Process:

Each Department must outline their end of day batch and reconciliation processes in their departmental processing procedures

The individual responsible for closing out all daily transactions must be designated by the campus merchant or delegate. A list of these individuals must be maintained by each campus merchant and be available upon request.

All credit card refunds should be processed and recorded as credit card refunds (not refunds via other mechanism).

If any consumer disputes (chargebacks) are received, the notice should be sent immediately to the Accountant in the Office of Revenue, Receivables, and Cashiering Services with a copy of the original transaction and an explanation of why the money should not be returned.

Individual(s) responsible for reconciliation must be designated by the campus merchant or delegate. A list of these individuals must be maintained by each campus merchant and be available upon request.

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 https://www.usg.edu/records_management/schedules/935.
- 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.

Technical Specifications

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

Systems Configuration

Campus merchants must work with the Office of Cyber Security to ensure that:

A. Anti-virus software is implemented and updated regularly on all systems and devices
B. Vendor patches are installed in a timely manner.
C. Data detection and data encryption software are implemented to ensure that all confidential data is identified, secured or deleted.
D. If external vendors or third-parties need access to service any third-party applications or software, access should only be granted for the time needed to complete the necessary task and then immediately disabled.

Incident Response Procedures

1. If the campus merchant suspects a potential privacy breach or tampering with a card terminal, contact Help Center with an emergency ticket.
2. The Cyber Security Office will activate the Cyber Security Incident Response Team (CSIRT) and notify the respective parties including Office of Revenue, Receivable & Cashiering Services.
3. When notified by the Cyber Security Office that the potential privacy breach Incident Response Plan has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of incident.
    a. Stop processing transactions or discontinue use of the machine /terminal in question
    b. Secure the scene: Do not disturb the terminal or network. Cyber Security team will investigate.
4. The Cyber Security Office will determine the scope of the potential breach and campus merchant will help to determine:
    a. Time Frame
    b. Specific Data Elements
    c. Specific Customers
5. The campus merchant will work with the Cyber Security Office to limit the exposure. Prevent further loss of data by doing the following:
    a. Do not access or alter compromised systems
    b. Isolate compromised systems from the network
    c. Preserve logs and electronic evidence
    d. Log all actions taken
    e. Be on high alert and monitor all systems
6. Report all findings to the Incident Response Plan Team.
7. The Office of Revenue, Receivable & Cashiering Services and the Cyber Security Office will assist the campus merchant in notifying the third-party vendor, if applicable.
8. The Cyber Security Office will contact the campus merchant services provider, University Legal Affairs Office and University Auditing and Advisory Services at this time.
9. The campus merchant will prepare a detailed written statement of fact about the account compromise.
10. The campus merchant will complete a list of all known potentially compromised account numbers and secure the information with their point of contact.

Forms/Instructions

Credit Card Authorization Form
Credit Card Merchant Application Form
Marketplace Access Request Form
Credit Card Terminal Return for Destruction

Additional Contacts

Office of Revenue, Receivable and Cashiering Services, 404-413-3251, rrcs@gsu.edu
Office of Comptroller, 404-413-3070, treasury@gsu.edu
Office of Information Security, 404-413-4357, security@gsu.edu
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, Vice President for Finance & Administration
Procedures Owner: Director of Revenue, Receivable & Cashiering Services
Procedures Contact: rrcs@gsu.edu
Phone Number: 404-413-3251

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 campus merchant is defined as a delegated representative from a department 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 who has obtained authorization from the CISO and Comptroller to process cardholder data.

Cardholder Data (CHD)*:* 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.

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 person as defined by the GSU Human Resources Policies and Procedures Employee Handbook.

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 stripes of the card.

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