### 5.1 Credit/Debit Cards

#### Policy Statement
The University is committed to safeguarding personal and account information conveyed in processing debit and credit card payments. Credit/Debit card payments are processed in compliance with Payment Card Industry (PCI) requirements which are intended to limit exposure and/or theft of personal cardholder information. To comply with these standards, it is the policy of the University that security standards relating to payment card transactions be specified and applied.

#### Reason for policy
The purpose of this policy is to establish a framework for processing payment cards, to safeguard against the exposure and possible theft of cardholder data received by the University of Georgia, and to comply with the current Payment Card Industry Data Security Standard (PCI DSS) requirements.

Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, fines imposed, and damage to the reputation of the department and university as a whole.

#### Procedures

**Scope of this Policy**

This policy applies to all units, affiliates, and employees of The University of Georgia, which accept, credit/debit payments in any form (electronic or paper). Relevant portions of this policy apply to all external organizations contracted by the aforementioned parties to provide outsourced services for credit/debit card process for University business and all third party vendors of the university accepting credit/debit card payments in any form (electronic or paper).

**Policy Specifications**

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

- The Vice President for Finance and Administration, Vice President for Information Technology or delegates must approve all credit/debit card-processing activities at the University of Georgia before a unit enters into any contracts or purchases software and/or equipment. Please refer to the Credit/Debit Card Processing Procedure section 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/debit card processing information with Bursar and Treasury Services.

- All technology implementation (including approval of authorized payment gateways) associated with the credit/debit card processing must be in accordance with The Credit/Debit Card Processing Procedures, PCI (Payment Card Industry) standards and the Board of Regents policies and approved by the VPFA, VPIT or delegate(s) prior to entering into any contracts or purchasing of software and/or equipment. Approved vendors and software must be confirmed as PCI compliant by the card associations and not just a third party assessor. Equipment must be validated as being PA-DSS compliant.

- Sensitive cardholder data should not be stored in any fashion on University of Georgia computers or networks. Transmission of sensitive cardholder data must follow guidelines for point of sale and ecommerce as described in the Credit/Debit Card Processing Procedures section. Credit Card point of sale receipts should follow approved procedures for storage and retention. Exemptions to this must be approved by both the VPFA and VPIT. The University does not allow the processing, storing or transmitting of credit card information on the university network unless approved by the Credit Card Committee via “Request for
Exception” or be an approved PCI P2PE solution that is listed on the PCI SSC’s List of Validated P2PE Solutions and comply with the requirements to complete a SAQ P2PE-HW.

- Any open communication system such as email or chat programs may not be used for the receipt or transmission of any credit card information.

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

- On an annual basis, the Chief Information Security Officer, Bursar and Treasury Services, Internal Auditing and/or the PCI Evaluator for the University will provide appropriate training to all employees associated with credit/debit card processing. Departments are required to send at least one employee to the training annually. However, each employee that is exposed to payment card processing should complete the signed PCI awareness/UGA Policy and Procedure acknowledgement form located on the Bursar and Treasury Services website at least annually and submit to the Credit Card Coordinator. This should also be completed if an employee transitions, or is hired, into a role that is responsible for handling payment card payments immediately upon hire or move.

- A background check is required, as a condition of employment, of any employee hired to be involved with credit card processing.

- All merchants must maintain and update departmental procedures for credit/debit card handling and processing. The procedure should be a reflection of how to properly handle all transactions within the department from start to finish. Procedure should also include proper retention information as well as destruction of unnecessary credit/debit card information.

- All units should create, maintain and test annually, business continuity and disaster recovery plans as well as incident response capabilities. Incident response procedures can be found in the Credit/Debit Card Processing Procedures.

- All servers and POS devices will be administered in accordance with the requirements of the Credit/Debit Card Processing Procedures. Departments operating point of sale equipment/software must follow the requirements section for “Equipment and Supplies”. General use is prohibited on any computer or electronic device used for Credit/Debit Card Processing (no email, web browsing or other unnecessary applications other than the web site related to the Credit/Debit Card processing). These reasonable measures include, but are not limited to, anti-virus software, firewalls, and automatic updating of the operating system. These systems must be registered with the Bursar and Treasury Services office before deployment and require the completion on the PCI DSS SAQ-VT yearly. The SAQ outlines the necessary requirements that must be followed in order for the Kiosk to be utilized. All Kiosk’s must be connected via DSL line only.

- Access to credit/debit card processing systems and related information must be restricted to appropriate full-time UGA personnel. These persons are defined as needing access to credit card information in order to perform their day-to-day job responsibilities.

- All departments accepting credit/debit cards for payment must comply with The University of Georgia Credit/Debit Card Processing Policy, Payment Card Industry (PCI) Standards, Board of Regents policy, and the University’s Customer Information Security Program (UGA Gramm Leach Billey Policy) to protect the private financial information of University customers. The Gramm Leach Billey policy is available at: [Gramm-Leach-Billey Act](https://www.gramm-leach-billey-act.com). The Office of Information Security’s website, [Office of Information Security](https://www.informationsecurity.uga.edu), may be referenced for additional information.

**C. The university will contract with an approved and certified PCI 3rdparty assessor to review our processes and determine any vulnerability as it relates to PCI compliance. Each unit responsible for credit/debit card processing must have a completed PCI DSS Self-Assessment Questionnaire, also known as an “SAQ”, on file with the approved assessor. This questionnaire needs to be reviewed annually to ensure compliance with this policy and the associated procedures and provide an update should current procedures/operations change. Each unit with the exception of point of sale merchants must also enroll and participate in quarterly network scans with the approved third party assessor. Each merchant’s questionnaire and scans will be documented and tracked by the approved third party assessor. Bursar and Treasury Services, Internal Audit and the Office of Information Security will have access to each merchant’s status on a continual basis. The Chief Information Security Officer and Bursar and Treasury Services will, at the request of the unit, assist in the initial PCI questionnaire. Audits will be performed periodically by the Internal Auditing Division to confirm the results of the PCI questionnaire.**

**D. Bursar and Treasury Services will monitor each merchant’s level of compliance yearly via the PCI compliance portal maintained by the University’s third party assessor.**
E. Should you become aware cardholder data has been compromised, you need to follow the incident response as outlined in the Credit/Debit Card Processing Procedures.

F. Third party service providers, including any software companies utilizing a payment gateway, are required to maintain PCI compliance and must complete the Contractual Addendum (UGA Merchant Using a Third Party Service Provider). An Attestation of Compliance (AOC) must also be sent along with the third party application for approval. If a payment gateway is selected, then it must be listed on the Visa Level 1 Global Registry of Service Providers.

G. Third party vendor merchants wishing to accept credit/debit card payments utilizing their own vendor merchant for any UGA departmental account must agree to the terms of the university’s PCI Contractual Addendum “PCI Contractual Addendum, Vendor Merchant” as well as maintain PCI DSS compliance Level 3 or better. An Attestation of Compliance (AOC) must be provided to the Credit Card Coordinator to be considered for this purpose.

H. Any third party vendor wishing to use the UGA network must submit a “Request for Exception” to Bursar and Treasury Services which will then be evaluated by the Credit Card Committee. If recommended for approval, the request must then be sent to the VPIT and VPFA for final approval. Third party vendors granted an exception approval must agree to comply with the “Minimum Security Standards for Sensitive Devices” in writing.

I. Retaining of credit/debit card numbers is not permitted unless it is a necessity of business. Regardless of full card number storage, at no time shall the CVC/CVV2 (three/four digit numbers on the back of a credit/debit card) be stored. Destruction of full card numbers should be done after a period of time when the information is considered no longer needed but no later than a twelve-month period. At such time, only a cross shredding machine can be used for destruction of information.

Revisions and Exceptions

This policy will 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 VPFA of The University of Georgia. The VPFA and the VPIT may grant exceptions to this policy or revise the Credit/Debit Card Processing Procedures by mutual agreement.

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 Guide to Progressive Discipline. Technology that does not comply with this policy and the associated required procedures is subject to disconnection of network services.

Credit/Debit Card Processing Procedures

A. Process to Implement Acceptance of Credit Card Payments

1. The following steps must be taken in order to implement payment card processing at the University.

   a. Read the credit card policy and procedures thoroughly.

   b. Complete and sign the Merchant Application located at: UGA Merchant Application

   c. Forward the application to the appropriate Dean/Director or Department Head.

      1. It is the responsibility of the Dean/Director or Department Head to approve the application. After the application has been approved, the application will be provided a merchant id and entered into the approved certified 3rdparty assessor system in order to complete a PCI DSS Self-Assessment Questionnaire, also known as a “SAQ”.

3. The Bursar and Treasury Services office will work with each merchant account regarding the purchase of all card processing terminals. Terminals must be connected via analog phone line.
4. If specialized software and/or systems are required, the Bursar and Treasury Services office will work with appropriate departments to ensure processing standards and safeguarding measures are met prior to purchase. Prior to purchase, the department must fill out the third party application for any software/systems which accept debit/credit payments.

B. Merchant Responsibilities

1. On a daily basis, the department must balance transactions and settle their sales electronically to the merchant services provider. The current merchant service provider for the University of Georgia is First Data and Sun Trust Merchant Services.

2. The department will complete the credit/debit card Web Departmental Deposit in the Cash Management System using the process UGA Cash Management System (Deposits). Receipts information for each deposit must be email to Bursar and Treasury Services so the sales revenue can be recorded in the University Financial Management System. Web Departmental Deposits summarizing the settled sales should be sent to Bursar and Treasury Services electronically no later than noon of the day following settlement. Merchants can access the credit/debit card sales transmittal form at: TouchNet Bursar and Treasury Services will reconcile the Web Departmental Deposit to the card processor and will immediately inform the department of any discrepancies. All discrepancies should be resolved within 24 hours so sales can be posted to the departmental account in the UGA Accounting System on a timely basis. All sales amounts will be reconciled to the bank account as well.

3. If Bursar and Treasury Services receives a chargeback or inquiry on a merchant account, the Credit Card Coordinator will contact the applicable department to provide support to dispute the chargeback.

4. Merchants are required to complete an annual SAQ and are subject to vulnerability scans if applicable. All results should be reviewed and any issues should be resolved within a week’s period. Should a merchant need an extension, a request should be submitted in writing to Bursar and Treasury Services with the reason and period for resolution.

5. Access to the physical location of stored credit card receipts should be in a restricted area where authorized persons can be easily identified and access to the area can be limited and restricted. Any visitors in this authorized area should always be identified, logged in and out and escorted at all times.

6. Cardholder information is not be taken or distributed for unauthorized purposes.

7. Each merchant ID assigned will have at least one person subscribed to the credit card listserv for updates on credit/debit card policy and procedures. Each merchant will also need to maintain their contact information in the portal of the PCI Evaluator for The University of Georgia.

C. Notification of Change of Merchant Account

1. Merchant departments must notify the Credit Card Coordinator prior to making any changes to initially approved method of processing. The changes should include but not limited to such actions as change in personnel that handle payment card processing, business process changes, or changes to equipment used to process payment cards.

D. Equipment and Supplies

1. Equipment for processing payment cards shall be PCI compliant and will be acquired through Bursar and Treasury Services.

2. A customer receipt must truncate the card number so only the last four digits are printed.

3. All POS terminals should be placed in a secure location and, if able, secured and locked away when not in use.

4. All phone based point-of-sale terminal transactions must be batched and transmitted to the card processor on a daily basis. Transmissions of sensitive cardholder data should be encrypted using PCI-DSS strong encryption and purged after settlement. All phone based point-of-sale terminals should be connected via Centrex AT&T analog phone line.

5. Those units, which utilize a fax machine for credit card orders, must operate a stand-alone fax machine connected via 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.

6. Any equipment no longer being used should be returned to Bursar and Treasury Services for proper disposal.

E. Software and E-Commerce
1. Bursar and Treasury 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 Bursar and Treasury Services.

2. A network diagram must be approved by the Credit Card Committee before a purchase of any system. “A data flow diagram (DFD) is a graphical representation of the “flow” of data through an information system, modeling its process aspects”.

3. Any software purchased to accept payment cards must be certified as PA-DSS and listed on the PCI validated payment application listing with appropriate version and type. Software purchases for payment card acceptance, even if they are not serving as a service provider, must also have the addendum "UGA Merchant Using a Third Party Service Provider" signed and included in their contract.

4. The recommended processes are the P2PE certified applications, listed on the PCI Security Standard Council List of Validated P2PE Solutions.

5. The University maintains a list of all service providers as well as require all service providers to have a written agreement in place that acknowledges that the service provider is responsible for the security of cardholder data that the service provider possess. The list of service providers is reviewed on a quarterly basis to ensure they are still located on the Visa Level 1 Global Registry of Service Providers. The Contractual Addendum (UGA Merchant Using a Third Party Service Provider) must be included in the contract when seeking approval as well as a diagram showing the flow of payment card information and all servers/networks associated. This requirement is applied to payment gateways as well.

6. The Unit/Department must contact the Office of Information Security which will conduct penetration testing on all proposed specialized software. The penetration test must meet the satisfactory approval by an EITS delegate and the Credit Card Coordinator prior to launching credit card acceptance.

7. Card processing transactions should be performed on the website of the payment gateway (i.e., the customer should enter cardholder data on a payment engine website) and not on the University computer or network resources.

8. All IP based point of sale devices and/or e-commerce 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 PCI-DSS strong bit encryption and purged after settlement.

F. Exception to Policy

1. In order to be granted an exception to the policy, please submit a “Request for Exception” word document with the information below.

Request should include:

- Reason for requesting exception
- Steps being taken to become compliant with the policy
- Date your division is expected to become compliant

Bursar and Treasury Services will work with the VPFA and VPIT to determine if an exception to the policy can be granted. Any merchants granted an exception must follow each detail specified in the PCI requirements and be assessed as PCI compliant by an external assessor at their own expense on an annual basis.

G. Technical Specifications

Each University unit processing credit/debit cards will be responsible for adhering to the credit card merchants’ data security programs:

- VISA CISP
- MasterCard SDP
- Discover Network Disc
- PCI Security Council

Any questions with regard to the technical specifications should be directed to the Chief Information Security Officer.

H. Compromise Incident Response Procedures
Should the department become aware that any cardholder data was subject to compromise, the department should follow the steps outlined below within 24 hours:

1. Alert the following immediately
   - University Office of Information Security
   - University’s Bursar and Treasury Services

2. Immediately work with the Office of Information Security to limit the exposure. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.
   - Do not access or alter compromised systems
   - Do not turn the compromised machine off; isolate compromised systems from the network
   - Preserve logs and electronic evidence
   - Log all actions taken
   - Be on high alert and monitor all systems

3. Bursar and Treasury Services will assist the merchant in notifying the 3rd party vendor if this is applicable.

4. Bursar and Treasury Services will contact its Merchant services provider. The Merchant services provider will assist Bursar and Treasury Services in contacting each Card Association’s Fraud Control Group and the local office of the Secret Service. Bursar and Treasury Services should also contact the University’s Legal Affairs Office and Internal Audit at this time.

5. Provide all compromised accounts to the merchant services provider and to any other agency/company as instructed by the merchant services provider and/or card associations.

6. Provide an Incident Response Report document to each Card Association within the timeframe they specify.

7. If required by the card associations, undergo an independent forensic investigation.

I. Merchant Card Acceptance Best Practices

1. In order to reduce fraud, credit card companies recommend the following procedures for processing cards when the card is present (i.e., face to face transaction):
   - It is recommended you ask for an ID 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 embossed 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 card sale is suspicious, make a Code 10 call to the voice authorization center for the card being used.

2. If cardholder information is taken over the phone or via fax (i.e., card is not present), in order to reduce fraud, the following guidelines are recommended:
   - 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 (Address Verification System-AVS)
   - Request the Security Code (the three digit code on the back of the card in the signature panel) and validate the code at the time of authorization either electronically (through the POS device) or by calling the credit
card automated phone system. This code should be destroyed via a cross shredding machine once validated; it should not be stored physically or electronically at any time.

- Get a signature for each delivery that is not the card member
- Maintain credit card receipts and all delivery records for the retention period as specified in record retention below.

3. To help reduce fraud, the following actions are recommendations for departments with POS equipment:

- Ensure POS terminal is placed in a secure location and, if able, secured and locked away when not in use.
- POS swipe terminals can be programmed to request an access code prior to processing a refund. This action adds an additional security measure for financial transactions dealing with credit card refunds.

4. If a client should send their credit card information to the department, the following steps should be taken:

1) Click “Reply” on the email.

2) Delete the credit card number from the original portion of the email.

3) In your response, Copy and paste the following:

   a. “Thank you for contacting (insert department or name). We appreciate your business, however as part of our compliance effort with the Payment Card Data Security Standard and our practice to protect all of our clients Personally Identifiable Information, we cannot process the Credit card information that you have sent through email. We ask that you use one of the accepted methods of processing the sale. Those methods are:

   - Our Online form at (http://xxxxxxxxxx.edu)
   - Mail
   - Phone
   - Fax to:

4) Then promptly delete the original email and empty the trash.

   a. Notify your IT department immediately to see if they have the ability to run a “SECURE DELETE” feature.

---

**Additional contacts**

Lauren Hofmann, Credit Card Coordinator, 706-583-8271

---

**Policy definitions**

**Account Number:** The unique number identifying the cardholder’s account, which is used in financial transactions.

**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.

**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/Debit Card Processing:** Act of storing, processing, or transmitting credit/debit cardholder data.

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

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.

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.

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/Debit Card Processing: Act of storing, processing, or transmitting credit/debit cardholder data.


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

Employee: Any employee as defined by the UGA Human Resource Policy & Procedure UGA HR Policy and Procedure

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

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

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.

Responsibilities

Responsible University Senior Administrator: Vice President for Finance & Administration

Responsible University Administrator: Associate Vice President - Finance Division

Policy Owner: Bursar and Treasury Services

Policy Contact: thodges@uga.edu

Phone Number: 706-542-6825

Responsibilities: It is the responsibility of the department to properly handle cash/checks within the department for accuracy of deposits.

Record Retention

Departments should maintain adequate records of the sales transactions. Daily sales totals, logs, etc. substantiating revenue should be stored for 5 years. Individual receipt slips and other documents with cardholder data should be stored in a locked filing cabinet or safe and only need to be retained for 12 months. BOR 0472-03-001
In order to dispute a charge, customers must report the item to the credit card company within 12 months of the date of sale. 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 Dates
Effective Date:
Date Last Approved:
Date of Last Review: 06/27/2018
Date of Approval:
Previous Version of Policy: