CLAYTON STATE UNIVERSITY CREDIT/PAYMENT CARD PROCEDURE AND POLICY

Clayton State University is committed to safeguarding personal and account information conveyed in processing debit and credit card payments. 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.

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. 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, and to comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements.

Policy & Procedures

1. **This policy and procedure applies to all forms of credit card processing whether existing, new or changed services on behalf of the University or by affiliates using University systems.** Credit card processing includes any payment card transaction (whether credit card, debit card, or other instrument linked to such a card) or other transmission, processing or storage of credit card data regardless of the means by which that transaction is actuated. This includes transactions initiated in-person, via the telephone or other telephonic means, in paper form, by US mail or other courier, through a terminal, kiosk, computer system, website, mobile device or any other means. This policy applies to whether the processing is performed by the University or by an outside party acting as a service provider to the University.

2. **This policy and procedure applies to all units, affiliates, and employees of the University, which accept, credit/debit payments in any form (electronic or paper).** Relevant portions of this policy may 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 (. e-commerce, POS device, or e-commerce outsourced to a third party - electronic or paper).

3. **All units that going forward (after the 2016 review) that wish to process credit card transactions must request approval of Business and Finance.** Units must complete the Request or Change Form before initiating any credit card transactions or making substantive modifications to their current acceptance. A valid business purpose must be established to support the proposed arrangements.

4. **All units that are approved for accepting credit/debit cards for payment must comply with Credit/Debit Card Processing Policy, Payment Card Industry (PCI) Standards, Board of Regents policy, and Gramm Leach Bliley**. This is to protect the private financial information of University customers.

5. **All units that wish to process credit card transactions must obtain a University credit card merchant ID account from the Bursar's Office.** Units within the University or affiliates using the University's systems may not negotiate their own contracts with credit card companies, processors, or external services that accept credit card payments on the University's behalf. A

University department accepting credit cards is deemed a credit card merchant. Only the Bursar's Office is authorized to issue University credit card merchant ID account numbers, which are required for University acceptance of credit card payments and to enable deposits through the Bursar's Office. University departments must comply with this policy and all related security policies in order to maintain their credit card merchant IDs. Credit card merchants are expected to protect cardholder data and prevent the unauthorized use of that data. (Cardholder data refers to information printed, processed, transmitted or stored in any form from a credit card. Cardholder data elements include the primary account number (PAN), cardholder name, service code, and expiration date. Units may retain only the first six (6) digits and/or last four (4) digits of the PAN, as these data are not considered to be cardholder data under PCI DSS.)

6. **All system and service components utilized for credit card processing must be purchased or acquired through an approved University vendor for such purposes.** The University has established contracts, incorporating the necessary security provisions, for many system and service components needed for the acceptance and processing of credit card transactions. All units processing credit card payments, e.g., through the World Wide Web, are required to use them. 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 approved by IT and Business & Operations -the Bursar or Controller 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. Equipment should be validated as being PA-DSS compliant. All servers and POS devices will be administered in accordance with the requirements of the Credit/Debit Card Processing Procedures.

7. **Credit card information is not accepted via e-mail, chat, etc., and units may not retain any paper records with credit card information.** Any associated paper or other records or reports containing credit card customer information shall not be maintained unless absolutely necessary as determined by the unit or divisions department head or Vice President or equivalent with Bursar/Controller approval. If absolutely necessary to maintain, the paper shall be stored in locked and secured cabinets. 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.

8. Access to credit card information and the processing of credit card payments should be limited to those individuals whose job requires such access. Sensitive cardholder data should not be stored in any fashion on University 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 Controller and unit VP.

9. **Departments are responsible for informing the Bursar's Office of all employees in their unit who accept or process credit card transactions and requiring their employees document they**

have read the university's PCI compliance policy, credit card policy and procedure and the department's requirements. All should 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.

10. **Departments who suspect a breach and/or fraud involving credit cards should contact the Controller or VP of Business Operations, Bursar and IT immediately.**

11. **Annual training is mandatory for any employee involved with credit card processing.** All employees involved in credit card acceptance and processing must complete an annual certification of compliance training. Additionally, new employees involved in credit card acceptance and processing must complete training before they can assume credit card acceptance and processing responsibilities in their area. Failure to complete training successfully may result in the loss of the merchant's ability to process credit card transactions. On an annual basis, the University will provide 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 Compliance Policy form located on the Bursar's website at least annually and submit to the designated office. This should also be completed if an employee transitions, or is hired, into a role that is responsible for handling payment card payments upon hire or move. A background check is required, as a condition of employment, of any employee hired into a CSU designated position of trust.

12. **Units are responsible for timely communication with the Bursar's Office or IT Services regarding any credit card inquiries or requests for information.** All university merchants must respond to communications from the Budget and Finance, Bursar's Office or IT Services regarding credit card processing in a timely manner, including any surveys, annual questionnaires, or other inquiries. Some of these communications may be date sensitive, and failure to respond appropriately within the period indicated may result in the loss of the merchant's ability to process credit card transactions.

13. **Units are fully responsible for any and all fees associated to the merchant ID.** The University is charged fees on all credit card transactions. At month end, these fees will be charged to the unit based on that unit's activity. Additionally, some service providers may impose annual, one-time, or other fees for their services, and these are the responsibility of the merchant department. Any fines or other fees and costs resulting from non-compliance with Payment Card Industry security standards, including but not limited to those resulting from breaches of security or failure to complete annual training, will be the responsibility of the department where the failure occurred.

14. **Non-compliance with this policy may result in termination of card processing abilities for the individual and/or unit.** Units or individuals found to be acting outside of this and related policies or establishing non-approved credit card processing arrangements will have their card

processing terminated, and the unit will be responsible for any costs associated with this failure. 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

15. **This policy will be reviewed and revised as needed according to new standards and laws.**

Credit/Debit Card Processing Procedures

A. Implementation of 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 Credit Card Request/Modification Form available from Budget and Finance. Forward the application to the appropriate Dean/Director or Department Head.

c. Forward the application to the Bursar's Office for review and approval.

1. After the application has been approved, the application will be provided a merchant id and added to the University's List.

2. The Bursar will work with each merchant account regarding the purchase of all card processing terminals.

3. If specialized software and/or systems are required, the Bursar's office will work with appropriate departments to ensure processing standards and safeguarding measures are met prior to purchase. Prior to purchase, if applicable, the department must fill out the third party application for any software/systems which accept debit/credit payments.

B. Department/merchant Responsibilities

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

2. All discrepancies should be resolved within 24 hours so sales can be posted to the departmental account in the Accounting System on a timely basis. All sales amounts will be reconciled to the bank account as well.

3. If the Bursar receives a chargeback or inquiry on a merchant account, the office will contact the applicable department to provide support to dispute the chargeback.

4. Departments are required to assist with the completion of 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 to be taken or distributed for unauthorized purposes.

C. Notification of Change of Merchant Account

1. Merchant departments must notify the Bursar 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. A Request form may be required to be approved.

D. Equipment and Supplies

1. Equipment for processing payment cards should be PCI compliant and will be acquired through Bursar's office.

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.

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 for proper disposal.

E. Software and E-Commerce

1. Budget & Finance 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/Controller or VP for Business & Operations.

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.

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 an annual basis to ensure they are still located on the Visa Level 1 Global Registry of Service Providers. The Contractual Addendum (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. IT can conduct penetration testing on all proposed specialized software.

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 ecommerce transactions must be batched and transmitted to the card processor. 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/Procedure

1. In order to be granted an exception to the policy, please contact the Controller to request an exception. They will be rare and the request will need to contain:

2. Reason for requesting exception; 2. Steps being taken to become compliant with the policy; and 3. Date your division is expected to become compliant. Bursar/Controller and IT will 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. 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 Controller

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 will assist the merchant in notifying the 3rd party vendor if this is applicable.

4. Bursar will contact its Merchant services provider. The department will assist Bursar in contacting each law enforcement and others as needed.

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 have the customer insert the chip or 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 unless a pin transaction.
- 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 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:// xxxxxxxxxxx.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.

Date of Last Review: 06/27/2018

Date of Approval: 7/22/19