Clayton State University's Payment Card Industry (PCI) Compliance Policy
Interim Policy

Clayton State University is considered a merchant because it accepts payment by credit card for specific services or products. As such, the University must follow the standards established by the Payment Card Industry.

This policy has been created to assist employees in understanding the importance of protecting cardholder data and informing employees about the new rules surrounding safeguarding information. The Payment Card Industry (PCI) was formed by the five major card brands (Visa, MasterCard, American Express, Discover and JBC International). This group established a standard set of guidelines around the handling of cardholder data by merchants. These guidelines make up the Payment Card Industry Data Security Standard (PCI-DSS) and provide merchants with rules for physical, application and network security, as well as security policy management, which merchants are required to implement and follow.

The Payment Card Industry Security Standards Council (PCI-SSC) is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. PCI-DSS includes technical and operational requirements for **security management, policies, procedures, network architecture, software design and other critical protective measures** to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

Penalties are enforced for violators.

A. Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses handles or maintains credit card information. Clayton State University employees include full-time, part-time and hourly staff members as well as student workers who access, handle or maintain records.
- Employees who contract with service providers (third party vendors) who process credit card payments on behalf of Clayton State.
- Employees who manage events and require payment processing capabilities.
- IT staff.

Reason for the Policy: The standards are designed to protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the University. This policy is intended to be used in conjunction with the applicable PCI-DSS requirements as established and revised by the PCI Security Standards Council.

B. Entities Affected by this Policy:

1. All departments that collect, maintain or have access to credit card information. All employees or other designated individuals that collect, maintain or have access to credit card information or University terminals must comply with the PCI policy.

2. Others who do not have access to credit card data but accidently gain access must immediately report that information to his or her supervisor, to security and to Budget & Finance.
3. Third Party vendors that process and store credit card information for Clayton State that have been approved to collect payments on behalf of the University will be asked to provide PCI-DSS Certificate of Compliance.

C. Access to POS (point of sale) or Card Swipe Terminals and Credit Card Information

Only employees authorized and who have a business purpose may have access to process credit card payments. All card terminals should be located in areas where they will be used during business hours.

1. Credit Card Processing

Cards may be accepted by phone, fax, in person, online or by mail.

a. If cards are accepted in person, the card should be swiped through the machine and not manually keyed in. If the card is received by phone, fax or mail, any paper documents containing credit card information should be limited to what is required to transact business. Once the authorization for the charge is received any paper documents containing credit card information must be shredded. If there is a reason to retain the information, it can only be retained for a maximum of 150 days, and you must notify the Budget and Finance Manager if you are doing this. After January 1, 2017 the maximum time period will be reduced to 60 days. Cardholder information must be kept in a secured, locked location, and only employees with a business reason may have access to the stored information.
b. If a debit card is presented, under no circumstances should the payer provide the PIN number to the person processing the card information.
c. Card terminals should be used for processing credit cards. Manual credit card machines that make an imprint of the credit card are not allowed. The full card number should not print on the receipt that is given to the cardholder or kept by the University. Only the last 4 digits may appear.
d. Web payments must be processed using a PCI-compliant service provider on computers belonging to a secure cardholder data environment. Credit card numbers must NOT be entered into a web page of a server hosted on the Clayton State network.
e. NO card information may be received via email. Email is not a secured transmission method. If an email is received, do not process the payment. Immediately respond to the sender that the payment cannot be processed with an email request. Be sure that you do not include the card number in your reply and once you have responded, delete the original email that contained the card information. ***When the University migrates to encrypted email this section will be revised.***
f. Employees are not allowed to log cardholder information into a computer or keep the information in a paper log. Again, receiving or recording of PIN numbers is forbidden.

g. Employees must properly handle and destroy all data. All physical cardholder data (e.g., paper documents) that is deemed not essential must be properly destroyed. All electronic storage data also must be properly destroyed if there is no business or legal reason for which it should be kept. Proper means of destroying hard-copy material include physical destruction, such as shredding, incineration, or pulping hard copy materials, so that cardholder data cannot be reconstructed. Electronic cardholder data must be rendered unrecoverable in accordance with industry-accepted standards for secure deletion. If storage of cardholder data is necessary for business or legal purposes, portable media used to store cardholder data, including hard-copy

material, must be secured –for example, stored in a locked office , drawer or cabinet.

2. Training

New employees that have access to cardholder information must receive training before being granted access. Periodic training will be done for all individuals having access to cardholder information and terminals. All individuals who will or have access must read and sign the PCI Compliance Policy and starting October 15, 2016 sign a copy of the policy.

3. Incident Response

All employees are responsible to report any incidents of credit card theft, credit card data breach, damage, fraud, etc. to their supervisor, Business Operations/Budget and Finance, IT and Public Safety if criminal.

4. Third Party Vendors (Processors, Software Providers, Payment Gateways, or Other Service Providers)

- Budget and Finance must be notified of each merchant bank or processing contract of any third-party vendor that is engaged in, or proposes to engage in, the processing or storage of transaction data on behalf of Clayton State—regardless of the manner or duration of such activities.
- Budget and Finance will ensure that all third-party vendors are asked to certify their PCI Compliance.
- Starting October 15, 2016 all contracts that are renewed or entered into must contractually require that all third parties involved in credit card transactions meet all PCI security standards and that they provide proof of compliance and efforts at maintaining ongoing compliance.
- Information must be maintained about which PCI-DSS requirements are managed by each third party provider and which are managed by Clayton State.

5. Self-Assessment

- Complete an annual self-assessment. The PCI-DSS Self-Assessment Questionnaire must be completed annually at the University level by the merchant account owner and anytime a credit card related system or process changes.
- Complete any required scanning of systems on a periodic basis.

Additional Resources

PCI-DSS Requirements and Security Assessment Procedures:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

PCI-DSS Quick Reference Guide Version
3.0 https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3.pdf