Ohio Administrative Code

Rule 3342-7-01.2 Administrative policy regarding credit card security.

Effective: June 13, 2025

(A) Policy statement. For the express purpose of protecting credit card account information stored or transmitted through university resources and in furtherance of the university's objective in maintaining secure financial transactions, this policy implements a university-wide compliance program regarding the security of credit card transactions.

(B) Scope. This policy applies to all transactions involving credit card account information ("cardholder data") processed by a university employee or any other person or entity accepting credit card payments on behalf of a university division, department, office, or entity, whether utilizing internal university processing systems or external third-party processing systems. This policy also applies to all merchants who have established accounts in university systems or other electronic financial processing systems where transactions on behalf of the university are conducted.

(C) Definitions

(1) Credit card. Refers to a credit, debit, or a pre-paid branded card issued by a financial institution.

(2) Cardholder data. For the purposes of this policy, cardholder data is any personally identifiable information associated with a specific cardholder, such as account number, expiration date, name, address, social security number, and card validation code or card identification number.

(3) PCI DSS. For the purposes of this policy, the term PCI DSS refers to the "Payment Card Industry Data Security Standard" which is a set of requirements designed to ensure that the university maintains a secure environment in the processing, storage, and transmission of cardholder data.

(4) Merchant. For the purposes of this policy, credit card merchants at Kent state university are those authorized departments and their users provided for under this policy who are authorized to accept credit cards in payment for products and services. All merchants must follow established proceses before being approved to engage in commercial or other transactional activities on behalf of a

university department, office, etc.

(D) Implementation.

(1) Oversight and responsibility. The division of finance and administration, in coordination with the division of information technology, will be responsible for the implementation and coordination of compliance efforts associated with and in furtherance of this policy. However, responsibility for continued adherence to this policy and to an environment of compliance regarding credit card transactions is shared by all university offices and employees of Kent state university. Oversight will include, but is not limited to, attention to the following standards:

(a) Maintaining a secure network and systems;

(b) Protecting cardholder data;

(c) Maintaining a vulnerability management program;

(d) Implementing strong access control measures;

(e) Regularly monitoring and testing networks; and

(f) Maintaining an information security policy.

(2) Minimum requirements for compliance. All university credit card transactions must adhere to the following provisions:

(a) Methods of transactions. Credit card transactions shall be processed in person, by mail, using using a secure PCI DSS compliant university-approved electronic application or device. Guidelines for processing credit card transactions for each of these methods are maintained in the bursar's office. Confirmation of PCI DSS compliant device is available upon request from the bursar's office. Cardholder data shall not be accepted or transmitted via email, facsimile, or by phone. If accepting credit card payments by phone is necessary and a justified business purpose, then such transaction must be done using a dedicated phone device approved by the division of information technology.

Cardholder data shall not be obtained or stored using card imprint machines.

(b) Receipts.Customer receipts, either printed or electronic, shall show only the last four digits of the credit card number.

(c) Storage. Cardholder information electronically or in written form on university information server, or systems, or physical locations to ensure the protection of the stored credit cardholder data.

(d) Authorized users Personnel authorized to accept , process, or manage credit card transactions are required to participate in training related to their specific responsibilities annually.

(3) Periodic review. The division of finance and administration, in coordination with the division of information technology, may at any time perform periodic compliance reviews, audits, or scans of any merchant approved to conduct credit card processing.

(4) Annual review.

(a) Processing procedures and protections under this policy shall be reviewed annually by the division of finance and administration, with assistance from all relevant university resources.

(b) Each merchant shall perform, with guidance from the division of finance and administration and/or the division of information technology , an annual review and may be required to assist in the completion of the PCI DSS annual self-assessment questionnaire as a prerequisite for each annual approval to continue credit card processing under this rule.

(c) The division of finance and administration shall coordinate the university's annual assessment to ensure adherence with this rule and associated compliance standards.

(d) This policy shall be reviewed annually by the division of finance and administration and a log showing the date of the review and the name and title of the person who completed the review shall be maintained in the office of the senior vice president for finance and administration.

(5) Training. All merchants, and individuals authorized to processes credit card transactions as part

of the merchant agreement, existing at the effective date of this policy and all new merchants approved by the division of finance and administration shall complete an approved training course regarding credit card transactions prior to conducting credit card processing . The training course will be administered and managed by the bursar's office. All merchants and individuals approved to process credit card transactions are required to complete this training annually in order to continue accepting credit cards.

(6) Third-party access. Any party contracted for services by the university that will have access to cardholder data or will perform transactions on behalf of the university utilizing cardholder data must contractually agree to:

(a) Adhere to all applicable requirements in the current version of PCI DSS applicable for their merchant level;

(b) Be liable for the security of the cardholder data;

(c) Notify the university of any breaches, intrusions, or potential compromises of cardholder data within seventy-two hours of discovery; and

(d) Permit periodic information security reviews by the university. The university department, office, etc. contracting with such third-party providers shall be responsible for notifying the bursar's office of any such planned agreements in advance of executing an agreement.

(7) Disposal of electronic equipment. In order to reduce the risk of the unauthorized release of cardholder data that may be contained on university equipment that is sold, disposed of, or otherwise discarded, all media connected to equipment used for processing cardholder data shall be securely wiped before leaving the university. The division of information technology is responsible for adopting the appropriate university standards under this paragraph.

(E) Unauthorized access and breach.

(1) Immediate notification. Any merchant or other individual that becomes aware of a breach or potential compromise of data shall immediately notify the bursar's office and the office of security

and access management of such breach or condition. Please send this notification via e-mail to PCICompliance@kent.edu. At that time the university's incident response plan will be initiated as appropriate based on the specific circumstances.

(2) Incident response plan. The division of finance and administration and the division of information technology are responsible for drafting and maintaining an incident response plan to outline the university's official response in the event of a breach or other potential compromise of data or discovery of any condition of non-compliance. Upon notification by a merchant or other party of an event of breach, potential data compromise, or non-compliance, such plan shall be executed.

(3) Remediation. As a part of such plan, the division of finance and administration and the division of information technology will be responsible for jointly coordinating the university response and creating the remediation plan to restore compliance in accordance with this rule.

(F) Violation. University departments and/or merchants found in violation of this rule may besubject to various financial and other sanctions. These may include termination of merchant accounts, suspension of privileges to accept credit card payments, financial penalties and costs associated with a security breach including bringing a non-compliant application into compliance, and/or possible disciplinary action of the individual(s) involved - up to and including termination of employment.