Ohio Administrative Code

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

Effective: March 1, 2015

(A) Policy statement. For the express purpose of protecting credit card account information stored or transmitted through university resources and in furtherance of the universitys 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. For the purposes of this policy, the term credit card will also refer to debit card and pre-paid card transactions using branded cards including, but not limited to, American Express, Discover, Japan Credit Bureau, MasterCard, and Visa International.

(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 individuals provided for under this policy who may accept credit cards

in payment for products and services. All merchants must receive approval from the division of business and finance before engaging in commercial or other transactional activities on behalf of a university department, office, etc.

(D) Implementation.

(1) Oversight and responsibility. The division of business and finance, in coordination with the division of information services, 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 telephone, by mail, or 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 bursars office. Confirmation of university-approved applications is available upon request from the division of business and finance. Cardholder data shall not be accepted or transmitted via email or by

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

(b) Receipts. Printed customer receipts that are distributed to the customer or other internal or outside parties shall show only the last four digits of the credit card number.

(c) Storage. Cardholder data shall not be stored on university information server or systems. When storing written cardholder data, all but the last four digits of the credit card account number shall be redacted within sixty days, or as soon as refunds or disputes are no longer likely, not to exceed one hundred eighty days or as provided for in the university records retention schedule at http://www.kent.edu/generalcounsel/records/index.cfm.

(i) Paper records shall be stored in a locked room or cabinet to which only authorized employees are permitted access.

(ii) Merchants shall not store the credit card identification number in any form. The credit card identification number is the three-digit security code on the back of the credit card.

(iii) All merchants shall follow guidelines maintained in the bursars office and the university record retention schedule in the maintenance and destruction of any records related to credit card processing.

(d) Authorized personnel. Each merchant must designate specific authorized personnel who shall have access to cardholder data and such individuals will be required to participate in training related to their specific responsibilities annually.

(3) Periodic review. The division of business and finance, in coordination with the division of information services, 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 business and finance, with assistance from all relevant university resources.

(b) Each merchant shall perform, with guidance from the division of business and finance and/or the division of information services, an annual review and complete the PCI DSS self-assessment questionnaire as a prerequisite for each annual approval to continue credit card processing under this rule.

(c) The division of business and finance shall coordinate the universitys annual assessment to ensure adherence with this rule and associated compliance standards.

(d) This policy shall be reviewed annually by the division of business and finance 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 existing at the effective date of this policy and all new merchants approved by the division of business and finance shall complete a training course regarding secure credit card transactions prior to conducting credit card processing for transactions. Such training shall be an approved course as designated by the division of business and finance and completion shall be required 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 bursars

office of any such planned agreements in advance of executing an agreement.

(e) 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 office of security and access management 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 bursars 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 incident response plan shall be initiated as appropriate based on the specific circumstances.

(2) Incident response plan. The division of business and finance and the division of information services are responsible for drafting and maintaining an incident response plan to outline the universitys 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 business and finance and the division of information services 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 are subject 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.