3359-03-06 Acceptance of Credit Cards as a Payment Option to the University.

(A) The vice president for business and finance and chief financial officer, in addition to the duties and responsibilities set forth in university rules, is responsible for the administration and use of credit cards by all university offices that accept credit cards as a payment option to the university.

(B) Use of credit cards must be coordinated through the controller of the university of Akron. The university will determine which cards are acceptable to the university.

(C) Web-based card applications must meet the data security standards for storing, destroying and transmitting data. Such standards shall be determined according to the current applicable requirements of the respective credit cards, appropriate best management practices and such university requirements as may be applicable.

(D) Each department must complete a credit card merchant application to accept credit cards. This form will define what type of transactions will be accepted online, in person terminal or paper process. This request should also include the following: the item or service, the time frame for which the credit card usage is needed, the estimated volume, the account code to be charged for the bank charges (with the appropriate unit approvals), an the cash/credit control procedures in place in the department which comply with the cash/credit control policy, including how the equipment and credit card information will be safeguarded. Upon return of credit card merchant application and other appropriate information, the controller will review the information and contact the department to discuss options available based on volume, expense and frequency of need.

(E) When equipment and software is available, the controller will designate a contact person to set-up equipment; explain accounting procedures, credit card processing procedures and confirm security in place. Only upon such designation and final approval of the controller may the process of accepting credit card charges be commenced by university offices. Any independent arrangement whatsoever regarding credit cards or with any credit card processors is expressly prohibited.

(F) All staff with access to credit cards must acknowledge cash/credit card procedures for secure distribution and disposal of backup media and other media containing sensitive cardholder data.

(G) Information security polices are reviewed with staff at least once a year and updated as needed. All staff involved with accepting credit charges or information involving same shall be required to attend such training as may be directed.

(H) All employees with access to credit card/sensitive financial information may be required to have a basic background investigation.

(I) All cardholder data printed on paper or received by fax must be protected against unauthorized access. All third parties with access to sensitive cardholder data will be contractually obligated to comply with card association security standards.

(J) Security incidents should be reported by employees to their supervisor and the information security officer for a security investigation.