E-Commerce Procedure

Review www.bsu.edu/creditcards for up-to-date information, forms, and procedures.

THROUGHOUT THE YEAR

1. Prior to being granted access to CASHNet, ensure that all employees who need access to these systems have completed appropriate PCI training. Submit a list of any new employees to creditcards@bsu.edu for inclusion in training. Training dates/times must be recorded to ensure compliance with the University's Credit/Debit Card Handling Procedure.
2. Do not share any passwords related to CASHNet.
3. Do not input any credit card data into CASHNet directly. It is solely the customer's responsibility to input their payment information.
4. Do not indicate or set aside any Ball State computers as payment terminals. The University cannot guarantee any secure PCs or secluded network on which credit card data can be safely transmitted. If a customer is directed to a specific PC (or collection of PCs), it will be considered a virtual terminal and will put our entire computing infrastructure in scope for credit card fraud liability. However, if a customer happens to choose a University PC at random (without any direction whatsoever from our employees), then the customer is assuming liability upon themselves.
5. All online payments should be processed prior to the start of any event, or just before merchandise is being shipped out to the customer.
6. Any payments received in-person will be taken in cash or check form. If a customer wants to pay via credit card, we must adhere to procedure #4 above.

ANNUALLY

1. Complete the annual PCI Training for all employees that have access to CASHNet.
2. Review all of your departmental users in CASHNet with a member of the Financial Information Systems Department. They may contact you to initiate this process, but it is the department's responsibility to make sure no unauthorized employees remain in the system. All employees that remain in CASHNet must have completed their PCI Training to remain active.

CARDHOLDER DATA

1. Personal cardholder information (phone number, driver's license, full account number, card type, card expiration date, etc.) whether electronic or on paper should not be stored outside of the secure environment provided by CASHNet.
2. Retention of card verification codes (the three digit code on the back of credit cards) is strictly prohibited.