University Store Policies and Procedures (excerpt)

PCI Compliance

Credit card transactions are processed in-store using Verifone MX915 payment terminals. Customers may insert their chip-enabled credit card into the terminal or utilize the tap-to-pay function and follow the prompts to complete payment and sign. Employees should not handle customer credit cards or process payments on a customer's behalf for card-present payments.

In order to protect cardholder data, the following practices are in place:

- All credit card data provided through payment terminals, both online and in-store, are encrypted.
- Employees do not have access to encrypted cardholder data processed through payment terminals.
- Phone orders – When taking credit card information over the phone, the credit card number is entered directly into the MX915 terminal with the customer on the line. If a credit card number is written down on a phone order form, it is detached and shredded immediately upon successful payment.
- Any written credit card data obtained for non-returned book rental fees is kept in a locked safe with limited employee access.
- Any lost credit cards are kept in a locked safe with limited employee access for 24 hours, at which point they are shredded.

General Data Security

- Excluding designated stations, employees will log into computer terminals using their unique campus network user login and password.
- Employees that require access to the POS system user interface have a unique username and password that grants access to only the functions necessary to perform the assigned functions.
- Cashiers have been assigned a unique operator ID and pin to log into the register application.
- Personal usernames and passwords may not be shared.
- A user should log off a station if stepping away.
- Computer terminals will log off after five minutes of inactivity.
- Register applications will log off automatically after 4 minutes of inactivity.
- POS system passwords and register pins must be reset every 3 months and cannot repeat any of the previous 20.
- Campus network passwords must be reset every 6 months and cannot repeat any of the previous 20.