Security Awareness Program

All departments on campus that accept credit card payments via the web or in person using a terminal, must adhere to the CMU data security policies and procedures. All staff members who process credit card transactions must read and understand the following documents:

Merchant Sites Security Guidelines
Credit Card Security Training PowerPoint
The information Security Policy (3-42)

A Merchant Services staff member visits each merchant account annually to confirm this training is completed. The annual site visit includes but is not limited to:

1. A questionnaire that is completed by the Merchant Account Manager and includes a list of all staff member who process credit card transactions, and confirmation that they have been trained.

2. An inspection of all credit card terminals, devices and cables.

3. A review of each locations credit card procedures and documentation of any changes in equipment or procedures since the last visit.

4. A review of the incidence response plan in the event credit card data or equipment has been compromised.

Along with the annual visits, informational e-mails are forwarded to all Merchant Account Managers on a quarterly basis or more frequently as relevant information becomes available.

A Merchant Services staff member will also visit merchant sites during the year to update, maintain and troubleshoot equipment, review third party software changes and generally review security policies as the need arises.