Securing Your Point-of-Sale, Handheld Terminals and Cash Registers

All University merchants who use Point-of-Sale and Swipe Terminals to accept credit and debit card payments must follow common procedures to ensure the security of your terminal.

1. When register or terminal is not attended, make sure no person can access use of the terminal. If it is a handheld swipe terminal, it should be locked away in a secure environment. Cash register operators should never allow anyone to use their register while they are still logged on. Each cashier must have their own log in information and should log out whenever they step away from their station.
2. Only allow individuals who have received PCI DSS training on securely accepting credit and debit cards to process card transactions.
3. Registers/terminals must be checked daily for signs of tampering:
    a. Verify model and serial numbers
    b. Does terminal appear to have been moved?
    c. Are tamper evident stickers intact?
    d. Are there any missing screws or new “labels” on the device?
    e. Be aware of the “normal” number of cables going in and out of the terminal and review the device to make sure there are no “new” cables connected.
    f. Are there any new pieces of equipment attached to the terminal?
    g. If there are cameras on the premises, can cameras see the terminal? If so, is access to the recording devise controlled?
4. Ensure that authorized support personnel and technicians are escorted and monitored at all times while attending to the equipment.
5. If you believe a terminal may have been compromised, replaced, modified, removed or stolen you should
    a. Stop using terminal immediately
    b. Notify supervisor
    c. Appropriate supervisor, manager or administrator should contact Finance immediately at one of the following.
        i. Ginny Proctor Ext. 2434
        ii. Steven Heath Ext. 7594
        iii. compliance@sandiego.edu
        iv. Public Safety during non-business hours Ext. 7777

University of San Diego

This document is to be used by departments that use Point-of-Sale (POS) registers, handheld terminals or similar devices to process in-person/card present payments or card not present/manual entry transactions. Document should be retained and available for submission annually or upon request.

Department Name:

Merchant ID #

Device Location:

Device ID/Model #:

	Indicate that each area was reviewed with a Y or N							
Name	Date	Serial Number match?	Model number match?	Tamper Evident Stickers intact?	Foreign Object Attached to device?	Pry Marks or Bent, Broken, or Stressed Seams?	Unusual, damaged or missing wire connections?	Anything unusual?
Sam Smith	*5/22/2015*	*Y*	*Y*	*Y*	*N*	*N*	*N*	*N*