Securing Your Dial-up, or Wireless, Handheld Terminal

All University merchants who use dial-up or wireless, handheld terminals to accept credit and debit card payments must follow common procedures to ensure the security of the terminal.

- Dial-up and Wireless credit card terminals should be stored in a secure space accessible only to those authorized to process payment card transactions.
- Before using the device the first time in a day, examine the device and complete the log sheet. You are only required to complete the log on days transaction are processed. If you would like, you can log “no transactions” on days when no transactions are processed.
- The log document should be retained and available for submission annually or upon request.

If you believe a terminal may have been compromised, replaced, modified, removed or stolen you should:

1. Stop using the terminal immediately
2. Notify supervisor
3. Appropriate supervisor, manager or administrator should contact Finance immediately at one of the following.
    a. Ginny Proctor Ext. 2434
    b. Steven Heath Ext. 7594
    c. compliance@sandiego.edu
    d. Public Safety during non-business hours Ext. 7777

The following pages are to assist with the inspection of your equipment.

Check that manufacturer signage is visible and no object has been placed over the device.

Verify serial number, model number and any other identifying information is correct.

Check for pry marks, bent, broken or stressed seams.

Make sure tamper evident stickers are intact and there are no unusual or missing screws or wire connections and merchant ID # is correct.