

Tamper Prevention Inspections for Payment Card Terminals or Processing Device (perform quarterly)

Department:	
Staff Member Performing Inspection(s):	
Staff Member's Signature and Date of Inspection	

- A. All terminals and devices should be inspected quarterly and records maintained for internal and external auditors. This includes devices attached to an iOS phone or tablet.
- B. **Terminals with separate pin pads must be inspected as though they were two separate terminals.** (describe the base station in the Terminal 1 column and the pin pad in the Terminal2 column)

<u>TERMINAL or DEVICE DESCRIPTION</u>	<u>TERMINAL or DEVICE 1</u>		<u>TERMINAL or DEVICE 2</u>	
1. Serial number	1. _____		1. _____	
2. Make & model	2. _____		2. _____	
3. Location of terminal or device	3. _____		3. _____	
4. Color, size, condition & markings	4. _____		4. _____	
5. Security seals	5. _____		5. _____	
6. Cords – Color, number, & condition	6. _____		6. _____	
7. Number of connections or ports	7. _____		7. _____	
8. Manufacturer's security markings	8. _____		8. _____	
9. Describe device(s) attached or near the terminal	9. _____		9. _____	
10. Condition of ceiling (looking for potential camera installations designed to record payment card numbers and pin# during transactions)	10. _____		10. _____	
11. Number of Cameras (if applicable)	11. _____		11. _____	

	Yes	No	Yes	No
1. Is the serial number correct on the label and the screen?				
2. Are the terminal/device manufacturer's Make and Model correct?				
3. Is the terminal or device in its usual location?				
4. Are the color, size, and general condition of the terminal or device as described, with no additional marks or scratches (especially around the seams)?				
5. Are the manufacturer's security seals and labels intact?				
6. Are the cords/cables to the terminal/device as described using the same type and color of cables, with no loose or broken connections?				
7. Count the number of connections or ports to the terminal or device. Does this agree with the number stated?				
8. Are the manufacturer's security markings and reference numbers as described?				
9. Are all devices near or attached to the terminal or device as described and no new devices such as a skimmer?				
10. Is the condition of the ceiling above the terminal the same as described with no new marks, holes or fingerprints?				
11. If surveillance cameras are used, is the total number the same?				
12. Has the total number of terminals or devices changed?				
13. Have any personnel or third party requested access to troubleshoot, upgrade or change the terminal or device?				