The PCI Primary Department Contact is responsible for reviewing credit card processing terminal use by employees and ensuring the employees are following daily operations to identify if a device has been tampered with.

**Suspicious activity or identifying a device that appears to have been tampered with should be reported immediately to the Business & Finance and Information Technology departments.**

The following monthly tasks are required from each department primary PCI contact. Please check off verification of each step on the log sheet provided as this sheet will be reviewed annually by the Business & Finance department. Failure to maintain log files will result in loss of terminal.

1. Maintain a list of every device that is used within your department
2. Review the daily log sheet per device to ensure it is filled out by employees and that they are checking devices daily
3. Visually check the device(s) and compare it to the original picture provided to you upon purchase of the device
   a. Verify the Serial # on each device with what is on your inventory of devices
   a. Visually inspect the screw holes and/or plates to ensure they have not been tampered with
   b. No additional equipment/wires are hooked to the device
   c. Inspect keypad for fake overlays/keypads that seem thicker than rest of the terminal
   d. Inspect terminal for parts that do not match in styling, color or material
4. Check that each terminal securely locked up when not in use and when done processing for the day
5. Report any suspicious behavior to your supervisor and the Business & Finance office
6. If the primary PCI contact has changed, notify the Business & Finance office and Information Technology office of the change