

POS & EQUIPMENT DAILY INSPECTION CHECKLIST

(Opening / Startup Check)

Opening / Startup Check

Week of: Location / Register: Staff:

TASK	MON	TUE	WED	THU	FRI	SAT	SUN
Power on each POS terminal and confirm it boots fully to the sale screen with no error messages.							
Confirm the terminal is connected to the network / internet and the payment application is online.							
Test the barcode scanner on a known item; clean the scan window if reads are slow or failing.							
Load or confirm receipt paper and print a test receipt; check for faint or missing print.							
Open and close the cash drawer; confirm it triggers from the terminal and latches properly.							
Verify the card reader powers on and shows the ready/idle screen for chip, tap, and swipe.							
Confirm the starting cash float is counted, correct, and logged for each drawer.							
Check that the customer-facing display and any kitchen display / order screens are working.							
Confirm the date, time, and current pricing/promotions are correct on the terminal.							
Additional Task:							

Instructions:

Complete before opening at each register. Most POS failures during trading hours — a scanner that needs cleaning, a printer out of paper, a card reader that dropped its connection — are preventable with a five-minute morning check before the first customer arrives. A terminal that boots but can't reach the network can't process card payments, so confirm connectivity, not just power. Count and log every drawer's starting float so end-of-day reconciliation is clean.

POS & EQUIPMENT DAILY INSPECTION CHECKLIST

(Payment Device Security & Tamper Check — PCI DSS)

Payment Device Security & Tamper Check

Week of: Location / Register: Staff:

TASK	MON	TUE	WED	THU	FRI	SAT	SUN
Inspect each card reader / PIN pad for skimmers or overlays: anything added, loose, or not flush with the device.							
Check security seals and screws — broken seals, missing screws, or signs of a opened case indicate tampering.							
Inspect cables and connectors: look for swapped, added, or altered cables, or an unexpected inline device.							
Verify the card reader / PIN pad serial number matches your recorded device inventory.							
Confirm no unauthorized device (USB, adapter, wireless dongle) is attached to the terminal.							
Check that the terminal is physically secured to the counter and hasn't been moved or swapped.							
If ANY tampering is suspected, remove the device from service, do not process cards, and report it immediately.							
Confirm surveillance covers the POS area and is recording (without a camera aimed at the PIN pad).							
Additional Task:							

Instructions:

Complete daily at each payment device. PCI DSS requires periodic inspection of payment terminals for tampering, and daily checks are best practice — skimmers, overlays, and inline devices steal card data during normal transactions and are designed to look like they belong. Compare each device's serial number to your maintained inventory so a swapped device is caught immediately. Signs of tampering include broken seals, missing screws, and altered or extra cables. If a device looks tampered with, do not use it: take it out of service and report it before any more cards are run.

POS & EQUIPMENT DAILY INSPECTION CHECKLIST

(Closing / End-of-Day Check)

Closing / End-of-Day Check

Week of: Location / Register: Staff:

TASK	1ST	2ND	3RD	4TH	5TH
Run the end-of-day batch / settlement so the day's card transactions are submitted for funding.					
Confirm the batch settled successfully with no declined or unsettled transactions left open.					
Count each cash drawer and reconcile against the terminal's sales report; log any over/short.					
Record and secure cash per your drop procedure; leave the correct float or empty the drawer per policy.					
Print or export the daily sales / Z-report and file it for the day's records.					
Confirm the day's data has backed up or synced to the cloud / back office.					
Clean terminal screens, card readers, and scanners with an approved wipe (no harsh solvents).					
Lock or log out terminals and secure handheld / tablet POS devices in their charging dock.					
Note any device fault or error seen during the day for follow-up.					
Additional Task:					

Instructions:

Complete at close for each register. Settling the batch is what actually gets you paid – an unsettled batch means the day's card sales aren't funded, so confirm it closed cleanly. Reconcile every drawer against the sales report and log any over/short while the shift is fresh. Confirm the day's data backed up before terminals are shut down, and secure handheld and tablet devices so they can't walk off overnight. Log any fault noticed during the day so it's fixed before it disrupts the next shift.

POS & EQUIPMENT DAILY INSPECTION CHECKLIST

(Weekly & Periodic Maintenance)

Weekly & Periodic Maintenance

Month: Location: Manager / IT:

TASK	1ST	2ND	3RD	4TH	5TH
Reconcile the full device inventory: every terminal, PIN pad, handheld, and reader by serial number and location.					
Apply pending POS software and payment-application updates during off-hours; confirm firmware is current.					
Deep-clean scanners, screens, card readers, and printers; blow out dust from vents and printer paper paths.					
Test and replace low or aging receipt-printer components (cutter, ribbon) and restock paper supply.					
Review user accounts and access: remove former staff, confirm manager-override controls, and check for shared logins.					
Confirm antivirus / endpoint protection is active and updated on back-office POS computers.					
Verify network security: POS network segmented, strong passwords, and two-factor where supported.					
Test the backup: confirm data is backing up and can be restored; check the offline/backup transaction path.					
Additional Task:					

Instructions:

Perform weekly (some items monthly per your IT policy). Keeping an accurate device inventory is what makes the daily tamper check meaningful — you can't spot a swapped terminal without a known baseline. Apply software and payment-application updates promptly; outdated POS software is a common breach vector. Treat PCI DSS as the floor, not the goal: segment the POS network, enforce strong passwords and two-factor authentication, keep endpoint protection current, and verify backups actually restore, not just run.

POS & EQUIPMENT DAILY INSPECTION CHECKLIST

(Documentation & PCI Compliance)

Documentation & PCI Compliance

Date:

TASK	STATUS
Maintain a device inventory: make, model, serial number, and location for every payment-capable device.	
Keep a daily tamper-inspection log with staff initials for each payment device.	
Record daily batch settlement results and cash reconciliation (over/short) per register.	
Log all POS/payment-application updates and firmware versions with dates.	
Document any suspected tampering or skimmer, the device removed, and the incident response taken.	
Retain daily Z-reports / sales reports and backup confirmations per your record policy.	
Keep records supporting your PCI DSS Self-Assessment Questionnaire (SAQ) and any ASV scan results.	
Confirm an incident-response contact and procedure is documented and known to staff.	
Additional Task:	

Instructions:

Documentation supports both operations and PCI DSS compliance. PCI DSS expects a maintained inventory of payment devices, periodic tamper inspections, and a documented incident-response plan – the daily tamper log and device inventory are the practical proof. Merchants demonstrate compliance through a Self-Assessment Questionnaire (SAQ) or formal assessment, so keep update logs, scan results, and inspection records organized. If a device is ever found tampered with, a documented response – remove from service, preserve, report – limits the damage and shows due diligence.