PRO LINK SYSTEMS • FREE RESOURCE, NO FORM REQUIRED

Holiday Peak POS Hardening Checklist

Lock down your point of sale **before** the holiday freeze — so the season runs on the plan you set, not the incident you didn't. Aligned to public standards (PCI DSS v4.0 and CISA #StopRansomware). General guidance, not a compliance assessment.

Move one — Harden before the freeze

1. **Patch and update everything in the payment path** — terminals, registers, back-office servers, the payment application and its operating systems. Replace or isolate anything end-of-life.
2. **Segment the payment network** — keep cardholder systems separate from guest Wi-Fi, back-office PCs and the rest of the store.
3. **Require strong, phishing-resistant sign-in** — MFA on anyone who can reach or administer the payment environment, including vendors and remote-support tools.
4. **Remove standing and default access** — change default passwords, retire shared logins, cut access no longer needed. Least privilege, checked.
5. **Lock down remote access** — inventory every remote-support and vendor connection, disable what isn't needed, put MFA in front of what is.
6. **Turn on endpoint protection and logging** — EDR on managed devices and logging where the card environment can be watched.

Move two — Know your PCI obligations

1. **Know your scope** — everything that stores, processes or transmits cardholder data, plus anything connected to it. Segmentation keeps that scope small.
2. **Isolate the cardholder environment** — a clear boundary enforced by the network, not by hope.
3. **Log and monitor access** — keep records of who reaches the card environment and what they do.
4. **Control who gets in** — unique IDs, least privilege and strong authentication; no shared accounts in the payment path.
5. **Confirm your validation obligations** — know which SAQ or assessment level applies, and what your acquiring bank requires and when.
6. **Check your vendors** — confirm POS, processor and support-vendor responsibilities in writing.

Move three — Set a change freeze

1. **Define the freeze window** — mark the peak weeks as 'leave it alone' and make sure every team and vendor knows the dates.
2. **Write down what's allowed anyway** — agree who approves a security patch or true emergency exception, and how.
3. **Verify your backups by restoring them** — before the freeze, not during an incident. An untested backup is not a backup.
4. **Keep one tested way back** — a known-good recovery path for payment and back-office systems.
5. **Know who answers** — confirm the escalation path and who picks up the phone during the peak, before you need them.
6. **Plan the thaw** — decide when the freeze lifts and in what order deferred changes return.

The public standards this is built on. The PCI Data Security Standard (PCI DSS v4.0), published by the PCI Security Standards Council, sets requirements for organizations that handle payment cards. CISA's #StopRansomware guidance is the public playbook for reducing ransomware risk: patch, use MFA, segment networks, and keep tested, recoverable backups. This checklist references both qualitatively and does not reproduce or interpret specific requirement numbers on your behalf.

Pro Link Systems has kept Los Angeles businesses running since 1999, from Woodland Hills — in-house, US-based, answering the phone live, around the clock. Want a second set of eyes before the freeze? Book a free 30-minute pre-holiday security review at prolinksystems.com/contact or call 1-800-890-6133.