Hotel Gateway Security Checklist

A one-page hotel Wi-Fi security review for routers, firewalls and HSIA gateways

PEACEY SYSTEMS
peaceysystems.com

1. Patch and lifecycle

- ☐ Inventory every router, firewall, gateway and controller, with model and firmware version.
- ☐ Install critical security patches within one month of release (PCI DSS v4.0.1 Req. 6.3.3).
- ☐ Track vendor end-of-life and end-of-support dates; budget replacements before support ends.
- ☐ Replace hardware that cannot run a currently supported, fixed release.

2. Management access

- ☐ No SSH, web, API or proprietary admin service reachable from the WAN or guest networks.
- ☐ Management only from a dedicated admin subnet or a modern VPN, enforced in firewall rules.
- ☐ Disable default admin accounts; unique passwords of 12+ characters; MFA where supported.
- ☐ Disable unused services (bandwidth test, SOCKS/proxy, MAC-layer admin, legacy protocols).

3. Segmentation

- ☐ Separate VLANs for guest, conference, casting/IPTV, PMS/back office, payment and management.
- ☐ Default-deny between wireless networks and the cardholder data environment (PCI DSS 1.3.3).
- ☐ Client isolation on guest Wi-Fi; guests never reach PMS, payment or device management.
- ☐ Change wireless vendor defaults (keys, AP passwords, SNMP) at install (PCI DSS 2.3.1).

4. Detection and monitoring

- ☐ Scan for authorized and unauthorized wireless access points at least quarterly (PCI DSS 11.2.1).
- ☐ Alert on new admin accounts, configuration changes and unusual outbound transfers.
- ☐ Send gateway logs to central storage that an attacker on the device cannot erase.
- ☐ Monitor certificate expiry, captive portal availability and authentication failure rates.

5. Incident readiness

- ☐ Keep a known-good configuration baseline offline for every device.
- ☐ If compromise is suspected: isolate, preserve logs, factory-reset, rebuild, rotate all secrets.
- ☐ Never restore a backup taken from a possibly compromised device.
- ☐ Document escalation contacts for ISP, gateway vendor, card processor and brand IT.

6. Guest experience and compliance

- ☐ Captive portal and PMS authentication remain reachable under peak load.
- ☐ Per-plan and per-device bandwidth limits so heavy users do not degrade HSIA for others.
- ☐ Confirm current brand HSIA standards and PCI DSS scope with each franchise or brand team.
- ☐ Review this checklist after every major advisory and at least once a year.

Book a free 30-minute gateway health check

peaceysystems.com/contact | sales@peaceysystems.com

References: PCI Security Standards Council, PCI DSS v4.0.1 (June 2024), Requirements 1.3.3, 2.3.1, 6.3.3 and 11.2.1; MikroTik Documentation, "Securing your router"; CERT Polska advisory on MikroTik RouterOS (September 5, 2026).
This checklist is general guidance, not a PCI DSS assessment or legal advice. Version: October 10, 2026.
Peacey Systems is the North American ANTlabs distributor, providing premium 24/7/365 Tier 1 support and NOC services.