Hotel PCI DSS Checklist

A practical checklist for Ontario and Canadian hotels accepting card payments. Aligned to PCI DSS v4.0.1. Prepared by AutoSecure Communications.

1. Know your scope

- [ ] List every way you accept cards: front desk terminals, PMS, booking engine, OTA virtual cards, restaurant/bar POS, phone and email bookings.
- [ ] Confirm your SAQ type with your acquirer (common for hotels: B-IP, C, P2PE or D) and your annual validation date.
- [ ] Keep a current network diagram and card data flow diagram.
- [ ] Know which vendors touch card data (PMS, payment gateway, POS, booking engine) and keep their PCI attestations (AOCs) on file.

2. Stop storing card data you don't need

- [ ] Never store the CVV/security code, full magnetic stripe or PIN data, ever.
- [ ] No card numbers in PMS notes, guest profiles, emails, spreadsheets or paper folders.
- [ ] Retire paper credit card authorization forms, or store them locked and shred them on a schedule.
- [ ] Use tokenization through your PMS and gateway so card numbers are not kept on site.
- [ ] Turn off or secure fax-to-email and voicemail that may capture card numbers.

3. Separate the payment network

- [ ] Payment terminals and systems are on their own network segment, isolated from guest WiFi.
- [ ] Guest WiFi uses client isolation and cannot reach front desk, PMS or POS devices.
- [ ] Firewall rules allow only what payment systems need; segmentation is tested and documented.
- [ ] No default passwords on routers, firewalls, switches, access points or terminals.

4. Control access

- [ ] Every staff member has their own login: no shared front desk or manager accounts.
- [ ] Multi-factor authentication (MFA) for all remote access and for any access into the payment environment.
- [ ] Remove access the same day an employee leaves.
- [ ] Vendor remote access is off by default and enabled only when needed, then logged.

5. Keep systems patched and protected

- [ ] Front desk and back-office computers run a supported operating system (no Windows 10 without paid extended updates).
- [ ] Security updates applied promptly; anti-malware/EDR installed and monitored.
- [ ] Payment terminals inspected regularly for tampering or skimmers, with an inventory of serial numbers.

6. Scan, test and log

- [ ] Quarterly external vulnerability scans by an Approved Scanning Vendor (ASV), with passing results on file, if your SAQ requires them.
- [ ] Internal vulnerability scans and fixes, if your SAQ requires them.
- [ ] Logs from firewalls and key systems are kept and reviewed.

7. Train staff and document

- [ ] Annual security awareness training, including phishing and social engineering (fake 'IT support' and fake guest calls).
- [ ] Front desk knows never to take card numbers by email, chat or text.
- [ ] Written security policy and incident response plan: who to call if card data may be exposed.
- [ ] Complete and submit your SAQ and Attestation of Compliance on time each year.

Need help? AutoSecure Communications helps Ontario hotels reduce PCI scope, segment networks and pass ASV scans. Book a free assessment: **226-476-3358** | autosecure.ca/services/pci-compliance/

This checklist is general guidance, not a formal PCI assessment. Your acquirer and SAQ determine your exact requirements. PCI DSS is a standard of the PCI Security Standards Council.