

FREE TECHNICAL GUIDE

Hotel Cybersecurity Checklist

the complete guide

25 controls across identity, network, suppliers and compliance, with why each one matters, how to assess your operation and the steps to fix it.

25

controls

4

areas

2026

edition

hotelti.com.br/en

BEFORE YOU START

How to use this guide

Hotels connect the PMS, POS terminals, guest Wi-Fi, electronic locks and supplier systems on a single operational network. Each category below is an entry point or lateral movement path already confirmed in real hospitality incidents, and the 25 controls in this guide address the failures that recur in those incidents.

01

Identity and access

02

**Network and
infrastructure**

03

**Suppliers and
integrations**

04

**Compliance and
incident response**

How to work through the checklist

1. **Assess one item at a time:** each one includes a direct question to confirm whether the control already exists in your operation.
2. **Use the complexity label** to prioritise: start with the quick items, which are usually internal configuration changes at no extra cost.
3. **Treat project items as a plan, not an afternoon task:** they usually need budget, a supplier or a change in process.
4. **Review the guide every 6 to 12 months,** or whenever you change PMS, booking engine or payment provider.

● Quick: internal configuration change ● Medium: involves a supplier or a new process ● Project: needs budget and planning

01 Identity and access

Who can get into your systems, with which credentials, and for how long after they stop needing to.

1. Multi-factor authentication (MFA) enabled on the PMS, corporate email and admin dashboards

QUICK

WHY IT MATTERS

A username and password on their own are the most common cause of unauthorised access. A second factor means a leaked password alone is not enough for an attacker.

HOW TO ASSESS

Ask: if I knew an employee's password right now, could I log in to the PMS with nothing else?

HOW TO FIX

- Enable MFA in the PMS, email and VPN/remote access settings. Do not leave it optional
- Start with accounts that have admin or financial access
- Use an authenticator app instead of SMS wherever the system allows it

2. No logins shared between staff on PMS or POS systems

QUICK

WHY IT MATTERS

Shared logins make it impossible to know who did what, and impossible to revoke one person's access without affecting the whole shift.

HOW TO ASSESS

Check how many staff can recite the generic front desk or cashier password from memory.

HOW TO FIX

- Create an individual user for every employee in the PMS and POS
- Disable generic accounts such as "frontdesk" or "cashier1"
- Turn on per-user audit logging if the system offers it

3. Former employees' access revoked on the day they leave

MEDIUM

WHY IT MATTERS

High-turnover areas such as the front desk and seasonal staff are where this control fails most often, and where forgotten access stays active for months.

HOW TO ASSESS

Ask for the list of active PMS users and compare it with the current payroll.

HOW TO FIX

- Create an offboarding checklist covering the PMS, email, Wi-Fi, VPN and supplier systems
- Make access revocation a formal part of the HR process, not an ad hoc IT task
- Audit active users against current staff every quarter

4. Monitoring for leaked credentials or credentials exposed on the dark web

MEDIUM

WHY IT MATTERS

Many corporate passwords circulate in leaks from other services long before they are used against the hotel.

HOW TO ASSESS

Ask whether anyone has checked the corporate email addresses against a breach-checking service in the last 6 months.

HOW TO FIX

- Subscribe to or enable a leaked-credential monitoring service for the company's domains
- Set up an automatic password reset process when a credential is flagged

5. PMS and POS access restricted by role, with no admin permissions by default

MEDIUM

WHY IT MATTERS

The more people with admin access, the larger the surface for mistakes and attacks. Most roles do not need that level of permission.

HOW TO ASSESS

Count how many users have admin rights in the PMS today and how many actually need them day to day.

HOW TO FIX

- Apply the principle of least privilege: each role sees and changes only what it needs
- Document admin exceptions with a justification and a review date

6. OTA extranet accounts (Booking.com, Expedia and similar) protected with MFA, and staff trained against targeted phishing

MEDIUM

WHY IT MATTERS

Recent campaigns take over extranet accounts to send guests fake "booking reconfirmation" messages, and some trick staff into running malicious commands on their computer (a technique known as ClickFix).

HOW TO ASSESS

Confirm that the extranet of every OTA the hotel uses has two-step verification enabled, not just a password.

HOW TO FIX

- Enable the two-step verification offered by the OTA platform itself
- Tell staff never to copy and run commands or scripts received by email, chat or guest message
- Review regularly who on the team has extranet access

02 Network and infrastructure

How the PMS, POS, guest Wi-Fi and in-room devices talk to each other, and what separates them from an attacker.

7. Guest Wi-Fi segmented and isolated from the operational network and the PMS

PROJECT

WHY IT MATTERS

Without segmentation, a compromised device on the guest network can, in theory, "see" the PMS and the payment terminals.

HOW TO ASSESS

Ask your IT provider for the current network diagram and confirm that guest, operations and in-room devices are on separate VLANs.

HOW TO FIX

- Set up separate VLANs for guests, operations and in-room devices
- Block traffic between VLANs by default, allowing only what is strictly necessary

8. POS terminal network isolated, within the defined PCI DSS scope

PROJECT

WHY IT MATTERS

Terminals with P2PE (point-to-point encryption) encrypt card data at the moment it is read, so the full card number never travels unprotected across the hotel network.

HOW TO ASSESS

Ask your acquirer or POS supplier whether the current terminals are P2PE certified.

HOW TO FIX

- Isolate the POS network on its own VLAN within the PCI DSS scope
- Prioritise switching to certified P2PE terminals at the next contract renewal

9. Default credentials changed on TVs, locks and smart room devices

QUICK

WHY IT MATTERS

Every IoT device leaves the factory with a default username and password, often published in manuals available online.

HOW TO ASSESS

Try the factory default login on a sample device. If it works, the problem is real.

HOW TO FIX

- Change all default credentials before or immediately after installation
- Record where each credential is stored, with restricted access to that list

10. Active vulnerability scanning beyond a standard firewall and antivirus

MEDIUM

WHY IT MATTERS

A firewall and antivirus are the floor, not the ceiling. They will not warn you about an outdated or misconfigured system before someone exploits it.

HOW TO ASSESS

Ask when your network last had a vulnerability scan. If nobody knows, it has probably never been done.

HOW TO FIX

- Arrange regular internal and external scans
- Treat the findings as a remediation plan with deadlines, not a report to file away

11. Backups tested regularly, with a copy offline or isolated from the main network

MEDIUM

WHY IT MATTERS

A backup that has never been restored is an assumption, not a guarantee. A backup that is only connected to the main network is a target for the same ransomware.

HOW TO ASSESS

Ask when someone last restored a test backup, rather than just confirming that it "ran".

HOW TO FIX

- Test a full restore at least once a quarter
- Keep at least one copy offline or isolated from the main network

12. Endpoint detection and response (EDR) on front desk, back-office and finance computers

MEDIUM

WHY IT MATTERS

Traditional antivirus recognises threats that are already catalogued; EDR watches behaviour and can contain an attack in progress. It is now a common requirement from cyber insurers.

HOW TO ASSESS

Confirm whether the protection on your computers is traditional antivirus or an EDR solution with active monitoring.

HOW TO FIX

- Replace traditional antivirus with an EDR solution on the most exposed computers
- Make sure the alerts it generates are actually monitored, not just collected

13. Firmware on electronic locks and other IoT devices kept up to date

MEDIUM

WHY IT MATTERS

Vulnerabilities such as the one that affected millions of electronic locks worldwide, allowing any door to be opened with a cloned card, can only be fixed with a firmware update.

HOW TO ASSESS

Ask your lock manufacturer which firmware version is installed and whether any security updates are pending.

HOW TO FIX

- Follow the security bulletins from the manufacturer of your locks and IoT devices
- Make firmware updates a recurring maintenance item, not a one-off event after installation

03 Suppliers and integrations

A hotel is rarely compromised on its own. A supplier with poorly controlled access is one of the most common routes in.

14. Supplier contracts with clear security clauses and a right to audit

MEDIUM

WHY IT MATTERS

Without specific clauses, the supplier has no formal obligation on security, or to respond to an incident that affects the hotel.

HOW TO ASSESS

Reread the contracts with your three most critical suppliers (PMS, payments, Wi-Fi) and check whether they mention information security.

HOW TO FIX

- Include security clauses and a right to audit in new contracts
- Negotiate amendments to the most critical contracts already in force

15. Supplier access to the PMS and loyalty systems reviewed regularly

QUICK

WHY IT MATTERS

Suppliers change teams and scope over time, and access granted at the start is rarely reviewed afterwards.

HOW TO ASSESS

List every supplier with active access today and confirm that they still provide the service that justified it.

HOW TO FIX

- Review supplier access every quarter
- Remove access immediately when a contract ends

16. Integrations between the PMS, booking engine and distribution channels audited

MEDIUM

WHY IT MATTERS

Every integration is a data exchange channel, and integrations left active after a supplier change are a common and barely visible risk.

HOW TO ASSESS

Ask your PMS provider for the list of active integrations and confirm that all of them are still in use.

HOW TO FIX

- Audit all active integrations and switch off the ones no longer in use
- Confirm that each remaining integration uses its own authentication and encryption

17. Incident notification deadlines set in contracts with critical suppliers

MEDIUM

WHY IT MATTERS

If a supplier suffers a breach involving your guests' data, you need to know in time to meet your own legal deadlines.

HOW TO ASSESS

Check whether the contracts with critical suppliers set a specific deadline for notifying the hotel of an incident.

HOW TO FIX

- Include an incident notification deadline in contracts with critical suppliers
- Align that deadline with the time you need to meet your own legal obligations

18. A central record of which suppliers have remote access to the hotel's systems

QUICK

WHY IT MATTERS

Without this record it is almost impossible to answer "who else had access" in the middle of an incident, exactly when a fast answer matters most.

HOW TO ASSESS

Try to put the list together now: if it takes more than a few minutes or means asking several people, the record does not really exist.

HOW TO FIX

- Create a single spreadsheet or register with the supplier, system, date granted and reason for access
- Update it every time access is granted or revoked

04 Compliance and incident response

What to do before an incident involving guest data, and in the first days after one.

19. An up-to-date map of which guest personal data is collected and where it is stored

MEDIUM

WHY IT MATTERS

Without this map it is impossible to answer a data subject request or to assess the real impact of an incident accurately.

HOW TO ASSESS

Ask: could anyone today list, within an hour, every system that stores guest data?

HOW TO FIX

- Map every system that collects or stores guest personal data
- Update the map whenever a new system or integration goes live

20. An incident response plan that is documented and tested, not just written

PROJECT

WHY IT MATTERS

A plan that has never been rehearsed tends to fail exactly when it is needed most.

HOW TO ASSESS

Ask when the last incident simulation was run with the people who would actually carry out the plan.

HOW TO FIX

- Document the roles, owners and steps of the incident response plan
- Run at least one tabletop exercise a year with the people involved

21. PCI DSS scope defined, with the SAQ or QSA assessment up to date

PROJECT

WHY IT MATTERS

Choosing the wrong SAQ type is itself a compliance failure. A badly defined scope usually only comes to light when it is already too late.

HOW TO ASSESS

Confirm whether anyone has formally validated which SAQ applies to the way the hotel processes payments today.

HOW TO FIX

- Identify the correct SAQ with the help of a QSA or specialist
- Keep the validation current and review it whenever the payment flow changes

22. A procedure ready to notify the ANPD, Brazil's data protection authority, within the 3 business days required by Resolution CD/ANPD No. 15/2024

MEDIUM

WHY IT MATTERS

The deadline is short and runs from when the hotel becomes aware of the incident. Having a template ready and an owner named in advance is what makes it achievable.

HOW TO ASSESS

Ask who, today, would know exactly what to do in the first hours after an incident involving guest data is identified.

HOW TO FIX

- Prepare an ANPD notification template in advance
- Formally name the person responsible for deciding on and sending the notification

23. Phishing training updated to recognise AI-generated attacks

QUICK

WHY IT MATTERS

AI-generated phishing emails have fewer spelling and grammar mistakes and imitate the tone of real suppliers and OTAs more convincingly. Old, obvious examples no longer prepare the team.

HOW TO ASSESS

Check the date of the team's last phishing training and whether the examples used are still realistic.

HOW TO FIX

- Update the training material with recent examples, including booking and OTA scams
- Repeat the training regularly, not as a one-off onboarding event

24. Email authentication (SPF, DKIM and DMARC) configured on the hotel's domain

MEDIUM

WHY IT MATTERS

Without these records it is easier to forge emails that appear to come from your domain to deceive guests or suppliers.

HOW TO ASSESS

Run the hotel's domain through a free DMARC checker and confirm that all three records are configured.

HOW TO FIX

- Configure SPF, DKIM and DMARC on the hotel's domain
- Move DMARC gradually to enforcement (reject), not just monitoring

25. Security monitoring with 24/7 coverage, not just alerts that nobody reviews

PROJECT

WHY IT MATTERS

An alert raised at 2 a.m. on a Saturday is only worth something if someone sees it and acts before Monday.

HOW TO ASSESS

Ask who, in practice, monitors security alerts outside business hours, and what happens if nobody sees them.

HOW TO FIX

- Evaluate an MDR (managed detection and response) service with 24/7 coverage
- Define a clear escalation process for critical alerts outside business hours

NEXT STEP

Want a full assessment of your operation, not just the checklist?

HotelTI, the hotel technology specialist, helps hotels and hotel groups identify the controls missing from their operation and plan and coordinate the fixes without disrupting the hotel's daily routine.

Website: hotelti.com.br/en

Email: info@hotelti.com.br

Hotel cybersecurity: hotelti.com.br/en/cybersecurity

This guide is for general information only and does not replace a technical assessment of your specific operation. The legal deadlines mentioned reflect the legislation in force at the date of publication; always check the latest official source. © 2026 HotelTI.