Venue Security Checklist

The 360° self-inspection — the same points we use on paid audits.

How to use: tick what's in place. Anything unticked is a gap. Anything unticked twice in a row is a liability — fix it or get it scoped. Run it quarterly, and after any incident, renovation, or vendor change.

1 · PERIMETER & ENTRY POINTS

- ☐ All entry/exit doors have commercial-grade locks — tested monthly, not assumed
- ☐ Rear/service doors self-close and self-lock; propped-open doors are a written breach
- ☐ Key register maintained — every key accounted for, signed in/out, no 'spare under the sink'
- ☐ Locks re-keyed after any staff departure with key access
- ☐ Windows and skylights within reach of ground level are lockable and checked at close
- ☐ Loading dock / delivery access supervised during deliveries only

2 · CCTV & ALARMS

- ☐ Cameras cover every entry/exit, the bar/till area, and the safe — not just the front door
- ☐ Footage retained 30+ days and actually retrievable (test a playback this week)
- ☐ Recording system is password-protected, off the default admin credentials
- ☐ Camera system firmware updated in the last 12 months
- ☐ Alarm is monitored (not just audible) and the response contact list is current
- ☐ Alarm codes are individual per staff member — no shared master code

3 · CASH HANDLING

- ☐ Till limits set and enforced — excess cash dropped to safe during service
- ☐ Safe is rated, bolted, and on a time delay
- ☐ Two-person rule for cash counts and banking runs
- ☐ Banking runs vary in time and route
- ☐ Float reconciled at every shift change, discrepancies logged same-day

4 · CLOSING PROCEDURES

- ☐ Written closing checklist exists and is signed off nightly — not tribal knowledge
- ☐ Two staff minimum at close; nobody locks up alone
- ☐ Full venue sweep before lock-up: toilets, cool rooms, storerooms, car park
- ☐ All doors/windows physically checked — not glanced at
- ☐ Last-out staff confirm alarm set before leaving the premises

Venue Security Checklist

The 360° self-inspection — the same points we use on paid audits.

5 · POS & PAYMENT SYSTEMS — CYBER

- ☐ POS terminals on a separate network from guest Wi-Fi and office devices
- ☐ POS vendor access is unique per vendor account — no shared logins, no remote access left on
- ☐ Default passwords changed on every terminal, router, and back-office PC
- ☐ Automatic updates enabled on POS and back-office systems
- ☐ Card data is never written down, photographed, or emailed — ever

6 · GUEST DATA & WI-FI — CYBER

- ☐ Guest Wi-Fi is isolated from all business systems (separate VLAN/network)
- ☐ Booking/loyalty/member data held by third-party vendors — you know exactly who holds what
- ☐ Vendor breach history checked: ask each vendor ‘have you ever reported a data breach?’
- ☐ You can list every system that stores guest names, phones, emails, or IDs
- ☐ Access to member databases revoked same-day when staff leave
- ☐ Backups run automatically and a restore has been tested in the last 6 months

7 · STAFF & INCIDENTS

- ☐ All staff know who to call and what to do in the first 10 minutes of an incident
- ☐ Incident register kept — every event logged, however minor
- ☐ Staff trained to verify identity before giving out any guest or business information
- ☐ Written data-breach response: who you notify, in what order (OAIC obligations apply if you hold personal information)
- ☐ Security licences of any contracted guards verified on the NSW public register

WHY THIS MATTERS

In 2024, one technology vendor serving the hospitality industry was breached — 17 venues, 1.05 million patron records exposed. The venues didn’t choose the breach; their vendor did. Physical locks didn’t help. Sections 5 and 6 of this checklist are the ones most venues have never run.

SCORE YOURSELF: 35+ ticks = solid baseline. 25–34 = gaps worth fixing this quarter. Under 25 = exposed on both fronts — a professional audit will pay for itself.

Honour Guard — physical + cyber security. One audit, no blind spots.