

HOSPITALITY, TRAVEL & TOURISM CYBERSECURITY

Welcome guests. Keep their data safe.

Guest data protection, booking and payment security, Wi-Fi testing, SOC and brand monitoring for hospitality, travel and tourism.

Three questions every hospitality and travel leader should be able to answer

Could a phished extranet login reach our guests?

OTA and channel manager accounts without MFA let attackers message guests and collect payments in your name.

Where is every passport and card we have collected?

Identity and payment data spread across PMS, vendors and partners is what DPDP and PCI DSS will ask about.

If the PMS went dark, could we check guests in?

Ransomware has sent hotels back to paper keys and bills; manual playbooks and tested backups decide the outcome.

339 m

Marriott Starwood records (2018)

£18.4 m

ICO fine on Marriott (2020)

9.95 m

Foreign tourist arrivals, 2024

6 hours

Incident reporting to CERT-In

Built for every hospitality and travel company

Hotel chains and management companies · hotel owners and franchisees · online travel agencies and booking platforms · tour operators and destination management companies · restaurant and QSR chains · event venues and convention centres.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits
DPDP · RBI tokenisation · PCI DSS	Guest data from May 2027; no card storage; payment environment controls
Immigration law 2025 · GST · SEBI LODR	Form C within 24 hours; e-invoicing; quarterly disclosure (listed)

Guest data, bookings and payments, Wi-Fi, SOC, brand and vendors

Guest Data Protection

DPDP programmes and data mapping across PMS, OTA, payment and CRM.

Booking & Payment Security

Booking engines, apps, APIs, PoS and PCI DSS v4.0.1 readiness.

Wi-Fi Testing

Guest and conference Wi-Fi, captive portals, IoT and building systems.

24/7 SOC

Properties, platforms, extranets and vendors monitored; 6-hour reporting.

Brand Monitoring

Fake booking sites, impersonation and leaked data detected and taken down.

Vendor & Platform Assurance

PMS, channel manager and payment vendors assessed and contracted.

Choose your starting point

Foundation

Property IT and Wi-Fi assessment, booking and payment review, backup and recovery review, policy and crisis plan. For independent hotels, restaurants and tour operators.

Assurance

Booking engine, app and API testing, PCI DSS readiness and DPDP programme, annual audit, SOC with brand monitoring. For hotel chains, QSR groups and venues.

Continuous Resilience

Continuous testing and red teaming, loyalty and payment fraud analytics, SOC with hunting, Board and owner reporting. For listed groups, OTAs and loyalty platforms.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to CERT-In, DPDP, RBI tokenisation, PCI DSS v4.0.1, immigration reporting and brand standard expectations.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your properties, platforms, vendors and guest data flows. We will propose a practical assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: Marriott disclosures, UK ICO, Ministry of Tourism, CERT-In. Confirm obligations against the official instruments.