ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Airlines and Airports: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

01 ☐ Have we mapped every system needed to process passengers, bags and flights?

02 ☐ Do we know which critical systems are run by suppliers or shared with others?

03 ☐ Do we know every connection between our networks and other airport tenants?

ACCESS

04 ☐ Is phishing-resistant MFA used for administrators and remote access?

05 ☐ Do help desks verify identity strongly before resetting passwords or MFA?

06 ☐ Is call centre access to customer data limited and monitored?

NETWORK

07 ☐ Are passenger, operational, airside and corporate networks separated?

08 ☐ Is public Wi-Fi fully isolated from airport and airline systems?

09 ☐ Are supplier connections controlled and monitored?

DETECTION

10 ☐ Do we monitor our networks around the clock for intruders and data theft?

11 ☐ Would we detect unauthorised changes to scripts on our payment pages?

12 ☐ Do we track GNSS interference along our routes and brief crews?

RESILIENCE

13 ☐ Are backups of critical systems stored offline and tested?

14 ☐ Can we check in, board and handle bags manually for several days?

15 ☐ Do we have a plan if a shared supplier system fails?

RESPONSE

16 ☐ Do we have playbooks for ransomware, data breaches and supplier outages?

17 ☐ Have we agreed in advance who decides on reducing the flight schedule?

18 ☐ Have we run a joint exercise with airlines, handlers and suppliers in the last 12 months?

PEOPLE AND GOVERNANCE

19 ☐ Have frontline, call centre and help desk staff been trained on social engineering?

20 ☐ Does the board receive regular reporting on cyber risk, including supplier risk?