ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Pharmaceutical Companies: 20 Questions to Ask

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

VISIBILITY

01 ☐ Do we know where our most valuable research and manufacturing data is stored?

02 ☐ Do we have an inventory of manufacturing and lab systems, including software versions?

03 ☐ Do we know which suppliers and partners we can't operate without?

ACCESS

04 ☐ Is phishing-resistant MFA used for staff, administrators and partners?

05 ☐ Is vendor access to plants enabled only when needed and monitored?

06 ☐ Is access to sensitive research and trial data restricted and reviewed?

NETWORK

07 ☐ Is there a DMZ between corporate IT and manufacturing networks?

08 ☐ Could our plants keep running if corporate IT were lost?

09 ☐ Are unpatchable validated systems protected by other controls?

DETECTION

10 ☐ Do we monitor manufacturing networks as well as IT?

11 ☐ Would we detect large amounts of research or patient data leaving the network?

12 ☐ Would we detect tampering with batch records or quality data?

RESILIENCE

13 ☐ Are backups of IT, manufacturing and quality systems stored offline and tested?

14 ☐ Can we restore validated systems quickly after an attack?

15 ☐ Do we hold contingency stock or alternatives for critical supplies?

RESPONSE

16 ☐ Is the quality function part of our cyber incident response team?

17 ☐ Do we know how we would assess product integrity after an attack?

18 ☐ Have we run an exercise involving manufacturing and quality in the last 12 months?

PEOPLE AND GOVERNANCE

19 ☐ Are researchers and plant staff trained on phishing and data handling?

20 ☐ Does the board treat cyber risk as a risk to supply, quality and patients?