Endpoint Security Audit Checklist

20-Point Business Device Defence Audit

☐ Are all laptops inventoried?
☐ Are all phones with business access inventoried?
☐ Are all servers reviewed?
☐ Is antivirus/EDR active everywhere?
☐ Are software updates enforced?
☐ Are vulnerable apps reviewed monthly?
☐ Are local passwords strong?
☐ Is MFA enabled on business accounts?
☐ Are local admin rights restricted?
☐ Are devices auto-locking?
☐ Is disk encryption enabled?
☐ Are lost device procedures documented?
☐ Are remote staff Wi-Fi risks discussed?
☐ Are SMS/mobile phishing risks discussed?
☐ Are unusual MFA prompts escalated?
☐ Are suspicious device slowdowns reported?
☐ Is endpoint monitoring active?
☐ Is internal device policy documented?
☐ Is monthly endpoint review assigned?
☐ Would one infected laptop create broad business exposure?

Scoring:

17–20 = Strong endpoint maturity
12–16 = Moderate device exposure
0–11 = High internal compromise risk