Wireless Network Security Readiness Assessment Checklist

Mark each item:

- Yes
- No
- Needs Review

Wireless Visibility

1. We maintain an inventory of all wireless access points and SSIDs.
2. We know which devices connect regularly to each wireless zone.
3. Wireless-connected IoT and smart office hardware are documented.

Credential Governance

4. Wi-Fi credentials are rotated on a defined schedule.
5. Guest Wi-Fi credentials are not treated as permanent public information.
6. Former employees and contractors no longer retain wireless trust.

Segmentation & Architecture

7. Guest traffic is truly isolated from internal business systems.
8. IoT devices operate in separate wireless trust zones.
9. Vendor or temporary hardware does not sit on employee-trusted networks.
10. Internal administrative wireless interfaces are restricted.

Hardware & Firmware Discipline

11. Access points and routers are updated regularly.
12. Default admin credentials have been removed from all wireless hardware.
13. Legacy weak compatibility settings are reviewed and minimised.

Remote Workforce Wireless Risk

14. Employees receive guidance on home router and public Wi-Fi safety.
15. BYOD wireless access is governed by policy.
16. Remote device trust is reviewed regularly.

Monitoring & Detection

17. Unknown or suspicious wireless devices are monitored.
18. Rogue SSID or duplicate signal checks are performed periodically.
19. Wireless authentication anomalies are reviewed.

Human Security Discipline

20. Employees understand the risk of fake or cloned wireless networks.
21. Staff do not casually distribute business Wi-Fi credentials.
22. Unauthorised personal hotspots or routers are prohibited.

Governance & Review

23. Wireless security has a clearly assigned internal owner.
24. Wireless segmentation is reviewed as infrastructure changes.
25. Wi-Fi is included in broader cybersecurity planning.

SCORING GUIDE

Strong Maturity (20–25 Yes Answers)

Your organisation demonstrates healthy wireless governance, trust control, and active infrastructure oversight.

Moderate Exposure (11–19 Yes Answers)

Basic protections exist, but convenience-driven wireless habits still create meaningful attacker opportunities.

High Vulnerability (0–10 Yes Answers)

Your wireless environment likely operates on assumption rather than disciplined oversight and may contain multiple hidden access risks.