ranix

2026

THE NETWORK SECURITY CHECKLIST

SELF AUDIT YOUR NETWORK



www.ranix.net



Introduction

This practical self-audit for small and mid-sized businesses will help you identify your biggest exposures before an attacker does.

Most breaches don't start with a sophisticated hack — they start with something being skipped. Work through both sections with your IT team or provider. Anything left unchecked is a good place to start.

For convenience, the checklist is broken down into two sections: network infrastructure and policy best practices.

If, at the end of this document, you are not sure where to go next or you would like an expert to help walk you through, you can book a free 30-minute review at: **www.ranix.net**



NETWORK INFRASTRUCTURE

Check:

- [ ] Firewall firmware is on the latest recommended vendor-supported version, with a documented patch schedule.
- [ ] All routers and switches are running current, vendor-recommended firmware.
- [ ] Default admin credentials have been changed on every firewall and network device.
- [ ] Firewall rules are reviewed at least quarterly and unused/legacy rules are removed.
- [ ] Legacy firewall rules are disabled as and when a service is decommissioned.
- [ ] Management interfaces (web UI, SSH) are not reachable from the public internet.
- [ ] No ‘permit IP/UDP/TCP any any’ rule exists.
- [ ] Outbound traffic rules exist — not just inbound — to minimise data exfiltration paths.
- [ ] Guest WiFi is on a separate, isolated network segment from business systems.
- [ ] Unused ports on network routers/switches are disabled.
- [ ] Unused services on network devices are disabled.
- [ ] Remote access (VPN or otherwise) requires MFA and is logged.



POLICY BEST PRACTICES

Check:

- [ ] User accounts follow the principle of least privilege; staff have access only to what their roles require.
- [ ] Former employees' access is revoked on the day they leave, across every system.
- [ ] Network traffic and logs are actively monitored, not just collected.
- [ ] There is a documented process for checking vendor security advisories weekly.
- [ ] Alerts exist for unusual login attempts, after-hours access, or config changes on network devices.
- [ ] At least one backup copy of device configuration is stored offline, isolated from ransomware reaching it.
- [ ] A documented decommissioning process exists for all network equipment.
- [ ] A written incident response plan exists and has been reviewed in the last 12 months.
- [ ] A designated person (internal or outsourced) owns network security responsibility and is known to all staff.
- [ ] A written acceptable use policy exists and is signed by every employee.
- [ ] Endpoint protection (antivirus/EDR) is installed and up to date on every device.
- [ ] A password policy is used and password reuse across systems is prohibited.

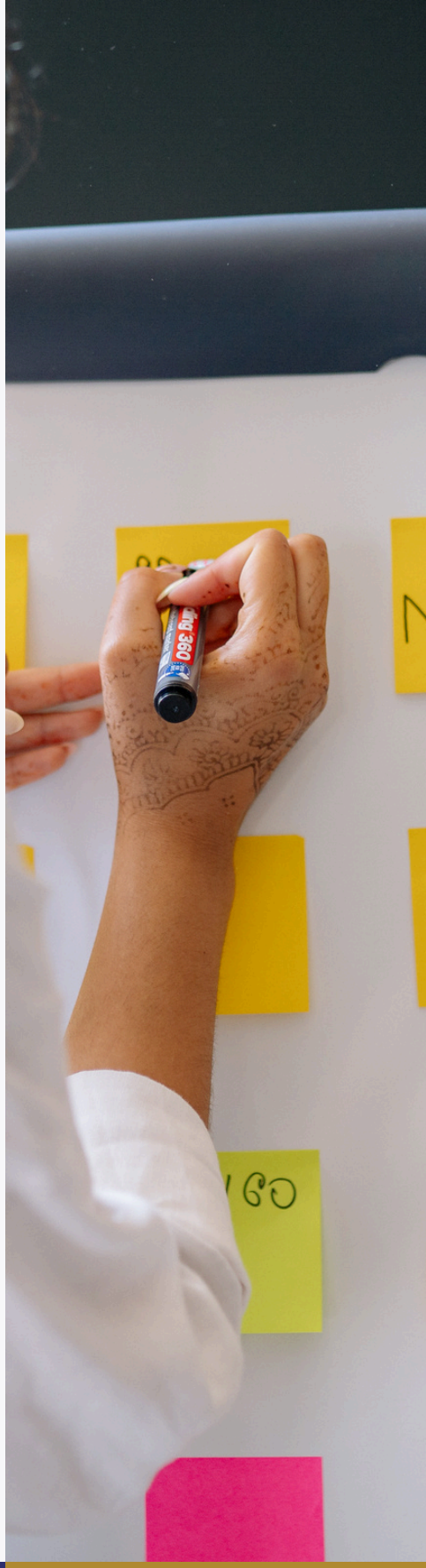


How many did you tick?

20–25: Strong posture - schedule a periodic review to stay there.
12–19: Real gaps exist - prioritise the unchecked items on page 02 first.
Below 12: Your business looks to be carrying significant, avoidable risk.

Want an expert to walk through this list with you? Book a free network security review at www.ranix.net

www.ranix.net



ranix

01530 686664

info@ranix.net