CORE NETWORK SOLUTIONS

Network health checklist

Twenty questions to find the weak spots in your network

Use this checklist to review your network in an afternoon. Every “no” or “don’t know” is worth looking into. Start with the ones that would stop your organization if they failed.

Documentation

- [ ] We have an up-to-date diagram of our network.
- [ ] We have a list of every switch, router, firewall and access point, with its location.
- [ ] Passwords and configurations are stored securely, and more than one person can reach them.
- [ ] We know who to call for each piece of equipment and each internet connection.

Lifecycle

- [ ] Every network device still receives security updates from its manufacturer.
- [ ] Firmware is updated on a schedule, not only when something breaks.
- [ ] We know when each device reaches end of support, and have a plan to replace it.

Resilience

- [ ] We know which single failures would stop the business: internet, core switch, firewall.
- [ ] Critical sites have a second internet connection, or a plan for when the first one fails.
- [ ] Configurations are backed up, so a failed device can be replaced quickly.

Security

- [ ] Guests, staff, servers and devices such as printers and cameras are on separate networks.
- [ ] Firewall rules are reviewed at least once a year, and unused ones removed.
- [ ] Remote access uses multi-factor authentication.
- [ ] Default passwords have been changed on every device.

Wi-Fi

- [ ] Wi-Fi works reliably in every area where people work.
- [ ] Staff Wi-Fi uses individual sign-ins or certificates, not one shared password.
- [ ] The guest network can't reach business systems.

Monitoring

- [ ] We're alerted when a device or connection goes down, before staff notice.
- [ ] Someone reviews the alerts and acts on them.
- [ ] We can see how busy our links are, and whether they're running out of capacity.

> **Next step**
>
> Not sure about some of these? A network assessment answers them for you, with a prioritized list of what to fix first.