# Secure Router Checklist

A quick-reference guide to lock down your network at the edge

### Hardware & Firmware

1 [ ] Router is not a consumer-grade model (e.g., no home use Netgear, TP-Link, etc.)
2 [ ] Device is still within vendor support and receives regular firmware updates
3 [ ] Latest firmware version is installed
4 [ ] Auto-update is enabled or checked at least monthly

### Access Control

1 [ ] Default admin username and password have been changed
2 [ ] Web interface is only accessible from internal network (not remotely)
3 [ ] SSH, Telnet, and UPnP are disabled unless explicitly needed
4 [ ] Guest WiFi is isolated from internal network via VLAN or separate SSID

### Monitoring & Alerts

1 [ ] WAN activity logs are enabled and stored for at least 30 days
2 [ ] Alerts for failed login attempts or WAN-based scans are turned on
3 [ ] Periodic review of logs is part of normal operations or vendor service

### Extras & Best Practices

1 [ ] Router is behind a UPS to maintain uptime during power loss
2 [ ] Inbound ports are blocked unless specifically required (e.g., VPN)
3 [ ] Device backup/export config is stored securely and updated after changes
4 [ ] End-of-life plans are documented with expected replacement dates

*Need help implementing these best practices? Wentz IT Consulting can assess and secure your entire edge infrastructure.*
https://wentzitconsulting.com/contact