Cybersecurity & Network Maintenance Checklist

Stay Secure, Compliant, and Confident Year-Round

Keeping your business safe isn't about one big project; it's about consistency.

Here's a quick checklist showing what IT teams and leaders should focus on daily, monthly, quarterly, and annually to stay protected and productive.

IT Administrator Checklist

Focus: System reliability, security controls, and network health. Prioritize automation where possible to free bandwidth for threats.

Leadership & Compliance Checklist

Focus: Security culture, visibility, and governance. Tie actions to KPIs (e.g., <5% phish click rate) for board-level buy-in. Foster "security as everyone's job."

Daily IT Admin	Daily Leadership & Compliance
☐ Review alerts from firewalls, EDR, and backups	☐ Share quick reminders or alerts from IT
☐ Verify systems and backups completed successfully	☐ Encourage staff to report phishing or anomalies
☐ Check VPN, email, and endpoint connectivity	
☐ Respond to any high-priority security notifications	
☐ Monitor bandwidth for unusual spikes	
☐ Log incidents or configuration changes	

Monthly IT Admin	Monthly Leadership & Compliance
☐ Patch and update endpoints, servers, and network devices	☐ Review metrics: phishing click rates, patch compliance, and incidents
☐ Validate backups with a test restore	☐ Verify staff training completion and engagement
☐ Review firewall rules and VPN access lists	☐ Ensure backups include all critical systems
☐ Audit admin accts and remove unused credentials	☐ Confirm incident response contact lists are current
☐ Run phishing simulations and assign new training	
☐ Update DNS filtering and antivirus definitions	
☐ Ensure all endpoint agents are active and reporting	

Quarterly IT Admin	Quarterly Leadership & Compliance
☐ Perform vulnerability scans across your network	☐ Meet with IT to review KPIs and overall risk posture
☐ Test your disaster recovery plan (failover or restore)	☐ Audit access controls and policy adherence
☐ Refresh network documentation and topology maps	☐ Check compliance readiness (HIPAA, PCI, NIST)
☐ Rotate privileged passwords and review third-party access	☐ Update internal security communications and policies
☐ Analyze security and performance trends for tuning	☐ Identify resource needs or skill gaps for cybersecurity initiatives
☐ Review endpoint and infrastructure capacity planning	

Annual IT Admin	Annual Leadership & Compliance
☐ Conduct a full security risk assessment	☐ Approve updated cybersecurity and continuity plans
☐ Schedule penetration tests or external audits	☐ Review cyber insurance coverage
☐ Evaluate network design — consider SASE or SD-WAN	☐ Conduct a tabletop exercise or breach drill
☐ Review and consolidate software licenses and SLAs	☐ Evaluate vendor contracts and renewal terms
☐ Update monitoring policies and alert thresholds	☐ Approve next year's security budget and roadmap
☐ Plan next-year IT and cybersecurity initiatives	☐ Refresh organization-wide awareness and training plan

Pro Tip

Juggling multiple IT and security tools drains time and resources. With TPx, you gain one partner to unify management across your infrastructure, enhance resilience, and free your team to focus on what drives the business forward.