



10 Signs It Is Time to Replace Your IT Provider

A decision guide for business owners who are tired of reactive support and avoidable technology problems.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



Use This Guide Carefully

Changing IT providers is a business decision, not just a technical decision. The goal is to reduce risk, improve responsiveness, and gain a partner that communicates clearly.

The 10 Signs

Done	Security Item	Why It Matters
[]	You only hear from IT when something breaks.	A good provider should be proactive, not purely reactive.
[]	Security recommendations are vague or missing.	The business needs clear guidance on MFA, backups, endpoint protection, and access control.
[]	Support tickets disappear without updates.	Communication matters as much as technical troubleshooting.
[]	Backups exist, but no one can prove restores work.	Untested backups are a business risk.
[]	There is no roadmap for Microsoft 365, cybersecurity, or infrastructure.	Technology should support business goals.
[]	You do not receive documentation for accounts, vendors, or systems.	Lack of documentation creates dependency and transition risk.
[]	The provider resists reasonable security controls.	MFA, least privilege, and patching should be standard conversation topics.
[]	Projects run late because planning is weak.	Execution needs ownership, communication, and follow-through.
[]	You are surprised by licensing, renewals, or hardware needs.	A provider should help with forecasting and budgeting.
[]	You no longer trust the advice you are receiving.	Trust is the foundation of a managed IT relationship.

What to Ask a Replacement Provider

- How do you document client environments?
- How do you handle MFA, admin access, and password management?
- How do you test backups and report results?
- What does your onboarding process include?
- How do you communicate ticket status and project progress?



Helpful Reference Points

- CISA says cybersecurity is about culture as much as technology and recommends leadership involvement, planning, and regular security objectives.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

