
VoIP Readiness Checklist

A business-friendly checklist to prepare your network, employees, phone numbers, and security controls for a cloud phone system migration.

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

Network Solutionist, LLC

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



Why VoIP Readiness Matters

VoIP and cloud phone systems rely on your internet connection, firewall, switches, call routing plan, security settings, and employee training. Preparing these items before migration helps reduce downtime, call quality issues, porting delays, and user frustration.

Readiness Checklist

Done	VoIP Readiness Item	Why It Matters
■	Confirm internet reliability and available bandwidth.	Stable upload, download, latency, and jitter are critical for clear voice calls.
■	Review current firewall and network switch readiness.	VoIP may require firewall adjustments, proper switching, and reliable internal network performance.
■	Configure Quality of Service where supported.	QoS helps prioritize voice traffic over backups, downloads, cloud sync, and streaming traffic.
■	Identify backup internet or failover options.	A secondary connection can help keep business calls active during an ISP outage.
■	Inventory all phone numbers and current carrier details.	Accurate billing and account details reduce number porting delays.
■	Document call routing, business hours, voicemail, and auto-attendants.	A written call flow helps avoid confusion during migration and go-live.
■	Identify analog devices such as fax, alarms, elevators, paging, or door systems.	Legacy devices may need adapters, replacement, or a separate service plan.
■	Plan remote worker, mobile app, softphone, and headset needs.	Hybrid users need reliable calling outside the office.
■	Enable MFA and restrict administrative access.	Cloud phone platforms should be protected like Microsoft 365 and other business systems.
■	Review international calling, fraud alerts, and calling restrictions.	Toll fraud can create significant expense if security controls are weak.

Documents to Keep Ready

- Recent phone bill and carrier account information.
- Inventory of all phone numbers, toll-free numbers, and fax lines.
- Network diagram or system inventory.
- Firewall, switch, and internet service details.
- Call routing, business hours, voicemail, and auto-attendant plan.
- Emergency calling and remote worker location notes.



Additional Readiness Items

Done	VoIP Readiness Item	Why It Matters
■	Review E911 and emergency location requirements.	Emergency calling must be planned for office users and remote workers.
■	Schedule user training and go-live testing.	Training and testing reduce disruption and help employees adopt the new system.

Admin Review Questions

- Who will own the phone system administrator role and backup administrator role?
- What happens to calls if the primary internet connection is down?
- Which analog devices still need support or replacement?
- Are emergency calling locations reviewed for office and remote users?
- Are users trained on voicemail, mobile apps, call transfers, and after-hours routing?

Helpful Reference Points

- Keep a recent phone bill available before number porting begins.
- Test inbound calls, outbound calls, voicemail, auto-attendant routing, groups, queues, and mobile apps before go-live.
- Backup internet and call forwarding procedures should be documented before a migration.
- Security controls should include MFA, restricted admin access, fraud alerts, and calling restrictions where appropriate.

Disclaimer

This guide is for general educational purposes and does not replace a formal network assessment, carrier review, compliance review, or emergency calling evaluation.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, migrate, monitor, and support your cloud voice, Microsoft 365, cybersecurity, backup, and managed IT environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

