NET-TECH CONSULTING

Real People, Real Protection, Right Now

Net-Tech MSP Core Services
The Four Pillars of Exceptional IT

Practical managed IT across Support, Devices, Security, and Backup & Recovery
Zero Trust security (ThreatLocker Gold Partner) + risk readiness add-ons available

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Why MSP Core Services matter now

Stability keeps teams productive. Security reduces exposure. Recovery keeps revenue moving.

Productivity breaks first

When support is slow, work stalls: password resets, email issues, app errors, VPN/Wi-Fi, printers—small problems that compound.

Device drift becomes downtime

Unpatched endpoints, aging hardware, and inconsistent configurations create outages (and security gaps). Device management prevents surprises.

Security needs control (not more tools)

Most incidents start with something “trusted.” Zero Trust reduces the blast radius by controlling what can run, connect, and move data.

Recovery + rehearsal matters

Backups only help if restores work. Tabletop exercises turn “we have a plan” into practiced response, owners, and follow-ups.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

What Net-Tech MSP Core Services are

A managed-services operating model that keeps your business productive, secure, and recoverable.

Net-Tech delivers a practical IT foundation—built on four pillars:

- End User Support (help desk + proactive guidance)
- Device Management (patching, monitoring, lifecycle)
- Security (layered security + optional Zero Trust control layer)
- Backup & Recovery (tested backups + restore readiness)
- Optional: Risk assessment + tabletop exercises for proof-ready resilience

Operator-built, right-sized for SMB + mid-market teams

Practical rollout

Onboard cleanly, stabilize operations, then tighten security controls—no “big bang” disruptions.

Minimal lift

We handle the day-to-day operations and documentation. Your team approves priorities and exceptions.

Proof of service

Clear tickets, asset inventory, patching history, and evidence exports—so you can answer audits, insurers, and customers.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

What you get (in plain English)

A stable IT operating model + security controls + proof you can reuse.

Core deliverables

Managed IT foundation across the four pillars

- End user support + ticketing
- Device monitoring + patching + lifecycle planning
- Layered security baseline + optional Zero Trust control layer
- Backup + recovery readiness (including restore testing)

Documentation that travels
(inventory + risk tracking + evidence exports)

Optional add-ons (when useful)

- ThreatLocker implementation + ongoing policy tuning
- Risk scorecard (20/30 control points) + 90-day action plan
- Tabletop exercise (incident response / ransomware / vendor compromise)
- vRC / vCISO governance cadence (quarterly risk reporting + evidence refresh)

NET-TECH CONSULTING
Real People, Real Protection, Right Now

How it works

Onboarding flow: stabilize → secure → prove → improve.

Stage 0: Onboarding

Kickoff workshop
Inventory + access
Support + escalation paths

Stage 1: Stabilize

Help desk live
Device monitoring + patching
Quick wins for uptime

Stage 2: Secure

Security baseline
Optional Zero Trust control layer (ThreatLocker)
Privileged access discipline

Stage 3: Recover + Prove

Backup/restore testing
Tabletop (optional)
Evidence + reporting cadence

Typical engagement cadence (fast and structured)

- Kickoff → scope and priorities
- Onboarding → support goes live, monitoring + patching begins
- Security hardening → baseline controls + Zero Trust (as needed)
- Recovery + proof → backup testing + evidence exports + tabletop (optional)
- Ongoing operations → quarterly risk review and continuous improvement

NET-TECH CONSULTING
Real People, Real Protection, Right Now

The Four Pillars of Exceptional IT

A balanced foundation: support, device management, security, and recovery.

Pillar I — End User Support

People-first help desk that keeps your team unblocked—fast response, clear communication, tracked tickets.

Pillar II — Device Management

Proactive monitoring, patching, and lifecycle planning so devices stay stable, current, and predictable.

Pillar III — Security

Layered security + optional Zero Trust control layer to reduce breach paths and limit blast radius—without tool sprawl.

Pillar IV — Backup & Recovery

Tested backups and restore readiness so you can recover quickly when hardware fails or ransomware hits.

We can right-size the pillars based on your needs today—then add maturity over time.
Rule: keep the foundation stable, then tighten controls and improve evidence.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Pillar I — End User Support (start here)

Fast, people-first support that keeps your team moving.

What's included

Help desk access, remote troubleshooting, and clear ticket ownership.
Common issues: accounts, email, printers, Wi-Fi/VPN, line-of-business apps.

How we deliver it

Modern ticketing + prioritization, documented resolutions, and escalation when needed.
We communicate in plain English—no runaround.

Result

Less downtime and fewer "small fires." Your team stays productive and confident.

Outcome: consistent support experience with visibility into every ticket.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Pillar II — Device Management

Proactive maintenance that prevents surprises.

What's included

24/7 monitoring, patch management, asset inventory, and endpoint standards.
Lifecycle planning so replacements happen before failures.

How we deliver it

Automated monitoring + scheduled maintenance windows.
Clear reporting on patch status, aging devices, and risk items.

Result

Fewer outages, faster performance, and a predictable device fleet your team can rely on.

Outcome: stable devices + fewer disruptions + fewer security gaps from drift.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Pillar III — Security (Layered + Zero Trust option)

Security that’s enforceable, not just “installed.”

Baseline security

Identity hardening (MFA/RBAC), firewall/AV, security awareness, and vulnerability tracking.

Zero Trust control layer

ThreatLocker (Gold Partner): default-deny application control, Ringfencing™, Storage Control, and Network Control.

Monitoring + response

Actionable alerting, documented incident process, and optional tabletop exercises to rehearse response.

Outcome: fewer breach paths and a smaller blast radius—with proof you can export.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Pillar IV — Backup & Recovery

A safety net that actually works when things go sideways.

What's included

Automated backups, encrypted storage, and retention aligned to business needs.
Offsite redundancy where appropriate.

How we deliver it

Monitoring of backup jobs + regular restore tests.
Recovery runbooks with clear restore priorities (RTO/RPO where defined).

Result

When hardware fails or ransomware hits, you can restore operations quickly with minimal disruption.

Outcome: tested restores + documented recovery steps + confidence under pressure.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Proof of service (audit / insurance / customer friendly)

We don’t just do the work—we show the work.

Service area	Typical proof artifacts
End user support	Ticket history, resolution notes, response metrics, and recurring-issue trends.
Device management	Asset inventory, patch status reports, lifecycle plan, and vulnerability tracking.
Security + Zero Trust	MFA/RBAC settings, ThreatLocker policy exports (allowlists, Ringfencing™, storage), exception history, and admin activity logs.
Backup + recovery	Backup job logs, restore test results, retention settings, and recovery runbooks.
Risk readiness (optional)	Risk scorecard + gap matrix, tabletop agenda/notes, after-action report, follow-up actions + owners.

Result: evidence that travels — leadership-ready, auditor-ready, and usable for customer security reviews.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

What we need to onboard smoothly

Minimal lift—just enough access and context to run the program cleanly.

People + context

- Primary IT point of contact + an executive sponsor
- Current pain points (support, downtime, security, recovery)
- Any compliance / insurance drivers (GLBA, PCI, HIPAA, SOC 2, etc.)

Tools + environment

- Endpoint + server inventory (or access to generate it)
- Identity provider details (SSO/MFA/RBAC)
- Backup platform details + current recovery expectations
- Vendor/remote access list (who connects, how, and why)

We can start even if parts are unknown—the kickoff workshop is designed to surface gaps and set priorities.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Kickoff workshop format (60 minutes)

Goal: align on priorities, onboarding plan, and what “good” looks like in the first 30–60 days.

1) Confirm operational priorities

What has to stay up? What can’t be disrupted?
Identify critical apps, users, and peak business hours.

2) Inventory + access

Endpoints/servers, users, identities, and vendors.
Confirm admin access paths and support escalation contacts.

3) Security + Zero Trust plan

Baseline security posture + decide where Zero Trust controls add the most value first (apps, elevation, storage, vendor access).

4) Recovery expectations

Confirm backup scope, restore priorities, and minimum recovery targets.
Optional: schedule tabletop exercise.

Pre-work (optional)

If you can share an asset list + vendor access list + current security stack beforehand, we’ll arrive with a draft onboarding plan.

NET-TECH CONSULTING
Real People, Real Protection, Right Now

How Net-Tech services fit together

MSP keeps operations stable. Zero Trust reduces exposure. Governance keeps it aligned and provable.

Layer 1 — Risk & compliance readiness (vRC / vCISO)

Risk scorecards, policies, evidence cadence, and leadership-ready reporting—aligned to your industry and insurer/customer requirements.

Layer 2 — Zero Trust technical controls (ThreatLocker + identity)

Default-deny application control, Ringfencing™, storage controls, elevation discipline, and vendor access governance—implemented and managed by Net-Tech.

Layer 3 — MSP operations (cloud + support + monitoring)

High-touch support, device management, cloud modernization, backup/recovery, and continuous maintenance that keeps the environment stable and scalable.

Adjacent: AI & Data Governance can be layered in when AI becomes an operational dependency (policies, boundaries, evidence).

NET-TECH CONSULTING
Real People, Real Protection, Right Now

Next steps

Let’s make the kickoff decision-ready and confirm the onboarding plan.

Checklist

- Confirm kickoff attendees (IT point of contact + executive sponsor)
- Share asset inventory (or grant access to generate it)
- Share vendor/remote access list (who connects, how, and why)
- Confirm backup scope + top 3 restore priorities
- Optional: schedule a risk scorecard + tabletop exercise

Contact: Zachary Kinder | Partner | zachary.kinder@net-tech.us | 877-449-8324