



APPALACHIA
TECHNOLOGIES

Prepared by:
Appalachia Technologies

*Your trusted technology advisor for
AI strategy, cybersecurity, and GRC*

Summer IT Survival Guide

How to Maintain Coverage During Vacation Season

The Problem You're Solving Right Now

Your ERP doesn't know it's July. Your security monitoring doesn't take weekends off. But your three-person IT team is about to.

If you're reading this, you already know the stress: someone's on vacation, a system goes down, and suddenly no one knows where the passwords are, who the vendor contact is, or what the actual recovery process is.

Vacation season is the stress test for your IT documentation and coverage planning.

This guide gives you a practical framework to maintain operations when half your team is at the beach without burning out the people who stayed behind.

WWW.APPALACHIA TECH.COM



The 4 Coverage Gaps That Surface in July (And How to Close Them)

1. Knowledge Gaps: “Only Sarah Knows How to Fix This”

The Problem: Critical knowledge lives in one person’s head. When they’re unreachable, you’re stuck.

The Fix:

- **Document the Top 5 Things That Break** — Password resets, VPN issues, email problems, printer failures, slow network. Write down the exact steps to fix each one.
- **Create a Contact Sheet** — Vendor names, account numbers, support phone numbers, escalation contacts. One page. Keep it current.
- **Test Your Documentation** — Have someone else follow your instructions. If they get stuck, your documentation isn’t done.

Quick Win: Block 2 hours this week to document just ONE recurring issue. That’s one less 2 a.m. panic call.

2. Monitoring Gaps: “We Didn’t Know It Was Down Until Monday”

The Problem: Monitoring tools don’t help if no one is watching them. Alerts go to inboxes no one is checking.

The Fix:

- **Audit Your Alert Routing** — Where do system alerts go? If it’s to one person’s email, you have a single point of failure.
- **Set Up Redundant Notification Paths** — Use a shared inbox or group text for critical alerts. If the primary person is out, someone else gets pinged.
- **Define ‘Critical’ vs. ‘Can Wait’** — Not every alert needs immediate response. Document which issues require after-hours action and which can wait until Monday.

Quick Win: Add one backup contact to your three most critical system alerts this week.

3. Incident Response Gaps: “What Do We Do If This Happens?”

The Problem: When something breaks, no one knows who has authority to make decisions or where to start.

The Fix:

- **Create a 1-Page Escalation Protocol** — Who gets called first? Who makes the call to take a system offline? Who contacts clients if there’s downtime? Write it down.
- **Pre-Authorize Recovery Steps** — Document which systems can be rebooted without approval, which require signoff, and who holds that authority when leadership is unreachable.
- **Rehearse Once** — Walk through one scenario: “The file server goes down on Friday at 5 p.m. Who does what?” If people hesitate, you need clarity.

Quick Win: Write down your escalation chain for one system—email, file server, or CRM.

4. Vendor Access Gaps: “We Can’t Reach Our Support Contact”

The Problem: Your MSP, software vendor, or hardware support is on summer hours too. Response times stretch. Projects stall.

The Fix:

- **Review Your Vendor SLAs Now** — What’s the guaranteed response time? Is 24/7 support actually 24/7, or business hours only? Know before you need it.
- **Confirm Backup Contacts** — If your primary rep is out, who covers? Get that name and number before August.
- **Front-Load Critical Projects** — If you’re planning infrastructure changes in August, move them to July or September. Don’t schedule major changes during peak vacation season.

Quick Win: Email your top 3 vendors today and confirm their August coverage plan.

4 Ways to Maintain Operations Without Burning Out Your Team

Option	Best For	Pro	Con
Rotating On-Call	Teams of 3+	Fair distribution	Requires cross-training
Stagger Vacations	Small teams (2-3)	Always someone available	Limits flexibility
Co-Managed IT	1-2 internal staff	Real time off	Requires planning
"Break Glass" Vendor	Budget-conscious	No additional cost	Longer response times

Your 1-Week Action Plan

You don't need to fix everything. You need to close your three biggest gaps before August.

This Week:

Monday: Identify your single point of failure. What breaks if one specific person is unavailable? Start documenting that system.

Wednesday: Audit alert routing. Add at least one backup contact to critical system alerts.

Friday: Confirm vendor coverage. Email your top 3 vendors and ask: "Who covers our account in August?"

Next Week:

- Test your documentation with someone else on the team.
- Write your 1-page escalation protocol.
- Decide on your coverage model and communicate it to the team.



When “Good Enough” Isn’t: A Reality Check

If any of the following are true, your current plan won’t survive August:

- You have one person who knows how to restart critical systems.
- Alerts go to individual inboxes, not a shared system.
- No one has tested your disaster recovery process in the last 12 months.
- Your team checks email or Slack “just in case” during vacation.
- You’ve delayed infrastructure projects because you can’t afford downtime during implementation.

That’s not a coverage plan. That’s a dependency.

Co-managed IT isn’t about replacing your team—it’s about extending capacity so your people can actually take time off without guilt or interruption.

What This Looks Like in Practice

A real scenario from a client (anonymized):

The Situation: Two-person IT team. Both wanted vacation in August. No formal coverage plan.

The Solution:

- Documented the 8 most common support requests (password resets, VPN access, email issues).
- Set up a shared alert inbox with escalation to an MSP for after-hours monitoring.
- Pre-authorized the MSP to restart specific systems without internal approval.
- Tested the process in July with one person on PTO.

The Result: Both IT staff took full weeks off. CEO never got a panicked call. The environment stayed stable.

The investment: 6 hours of documentation + co-managed monitoring contract.

Next Steps

If this guide surfaced gaps you didn’t know you had, you’re not alone. Most small IT teams are one vacation away from a coverage crisis.

Three ways to move forward:

Start Documenting

Test Coverage Plan

Explore Co-Managed IT

Appalachia Technologies has been providing co-managed and fully managed IT since 2004. We work with organizations in the 50-500 user range who need reliable coverage, clear documentation, and technology that just works.

We don’t drop tools and disappear. We build long-term partnerships with teams who want predictability, not surprises.