NETWORKS SOLUTIONS

AN EDUCATIONAL GUIDE
VOL. 01 · AEROSPACE

FOR AEROSPACE OPERATORS & MRO OWNERS

# The Aerospace & MRO Business Owner's Guide. To I.T. Support and Services.

The owner's guide to IT support for **Part 145 repair stations, AOG desks, parts distributors,** and aviation services businesses. What to pay, what to demand, and the 21 questions every aerospace operator should ask before signing.

**10+**
YEARS

**97%**
RETENTION

**24/7**
SOC SECURITY

**(844) 919-8534**
rrgnetworks.com

CONTENTS

# What's inside.

FROM THE DESK OF HEBER RODRIGUEZ, PRESIDENT

# Never ask an IT firm, "What do you charge?" Ask: "What will I get?"

If you own, run, or operate an aerospace, MRO, or aviation services business in South Florida — a Part 145 repair station, a parts distributor, an AOG desk, a component overhaul shop, a Part 135 operator — and you're looking to outsource some or all of your IT, this guide is for you.

I'm Heber Rodriguez, President of RRG Networks Solutions. We've served South Florida businesses for over 10 years with a 97% client retention rate. South Florida is one of the densest aerospace corridors in the country, and the IT challenges you face are not the same as a typical office. **You run 24/7 AOG desks. You handle controlled technical data subject to ITAR/EAR. Your repair-order, certificate-of-conformity, and 8130-3 records ARE the business — when they go down, you stop shipping.**

The most common question we get from prospects is "What do you charge?" — and it's the wrong question. The right question is what value you'll get for what you spend, and what risk you'll take on if you choose poorly.

I wrote this guide for three reasons:

**One:** to explain how IT firms package and price services, the pros and cons of each model, and which fits an aerospace business.

**Two:** to expose the contract clauses, hidden fees, and SLA gotchas that almost no aerospace owner thinks about until an aircraft is on a ramp at 2 a.m. and the ticket sits in a queue until Monday.

**Three:** to help you pick the right firm based on the value they deliver, not just the price — high or low.

My purpose is to help you make the most informed decision possible — so you end up working with someone who solves your problems on a timeline, in a manner, and within a budget that's right for you.

**Heber Rodriguez**
PRESIDENT · RRG NETWORKS SOLUTIONS

SOUTH FLORIDA'S AEROSPACE IT SPECIALIST

# The team behind 10+ years & 97% retention.

Fortinet-certified network specialists, a 24/7 Security Operations Center for security monitoring, and compliance-grade practices — built for aerospace operators who can't afford downtime.

RRG Networks Solutions is a leading network technology company serving South Florida businesses since 1999. We support clients across Miami-Dade, Broward, Palm Beach, Collier, Lee, and Monroe counties — including the dense aerospace cluster around **Miami-Opa Locka and the MIA cargo corridor.**

Our team includes full-time engineers and network specialists, supported by a 24/7 Security Operations Center for real-time threat monitoring. We're known for taking on complex environments — from a single-shop repair station to a multi-site MRO with multiple ERP integrations.

Our cybersecurity practice aligns with leading frameworks: **ISO/IEC 27001, NIST 800-171, PCI DSS, and HIPAA.** For aerospace clients, we extend this with ITAR access-control practices. Our security posture is audited recurringly by Galactic Advisors.

BY THE NUMBERS

## What 10+ years looks like.

**10+** — **YEARS IN BUSINESS**
Serving South Florida businesses.

**97%** — **CLIENT RETENTION**
Year over year. We earn it monthly.

**24/7** — **SECURITY OPS CENTER**
Real-time monitoring and response.

**9–5:30** — **OFFICE HOURS**
Live support Mon–Fri. After-hours emergency coverage available.

**Frameworks: FORTINET · NIST 800-171 · ISO/IEC 27001 · HIPAA · PCI DSS**

COMPARING APPLES TO APPLES

# Three ways to buy IT support.

Before you compare fees and SLAs, you have to know which model you're comparing. Most IT firms fit one of three approaches — and they're not interchangeable.

**Model 1 — Time and Materials.** The "break-fix" approach. You pay an hourly rate when something breaks. Useful for one-off projects when you already have a competent IT lead. Bad for ongoing operations: the firm has no incentive to prevent problems.

**Model 2 — Managed IT Services.** A flat monthly fee for an outsourced IT department. Includes monitoring, maintenance, antivirus, backups, and security. For aerospace operators, this is also where ITAR access controls, audit logging, and after-hours emergency response live.

**Model 3 — Vendor Help Desk.** Software vendors (Quantum Control, Pentagon 2000, AvSight, eMRO, Trax) offer per-app support. Great for the application — covers nothing else. Not a substitute for IT.

The two you're realistically choosing between: **managed services or break-fix.** Page 06 walks through which fits an aerospace business — and why "break-fix" works in the consultant's favor.

QUICK VERDICT

## Which model fits aerospace?

★ **TIME & MATERIALS**
One-off projects only. Bad for ongoing ops.

★★★ **MANAGED IT SERVICES**
Recommended. Predictable cost, proactive defense.

★ **VENDOR HELP DESK**
Useful add-on, never a replacement.

BOTTOM LINE

**For 24/7 aerospace operations, managed services is the only model that aligns the IT firm's incentives with yours.**

AN OUNCE OF PREVENTION

# The break-fix conflict of interest.

Under a break-fix model, the IT firm has no incentive to prevent problems, stabilize your network, or resolve issues quickly — they're **paid by the hour when things stop working.** The more problems you have, the more they profit.

## MANAGED IT SERVICES VS. BREAK-FIX

| | MANAGED IT | BREAK-FIX |
|---|---|---|
| COST | ✓ Flat monthly fee | ✕ Wildly variable hourly |
| INCENTIVE | ✓ Prevent problems | ✕ Profit from problems |
| RESPONSE TIME | ✓ Guaranteed in writing | ✕ Whenever they get to it |
| MONITORING | ✓ Yes — 24/7 proactive | ✕ No monitoring |
| CYBERSECURITY | ✓ Layered defense built-in | ✕ Reactive at best |
| AOG / AFTER-HRS | ✓ Covered in plan | ✕ Premium overtime rates |
| BEST FOR | ✓ Ongoing operations | ✕ One-off projects only |

RECOMMENDATION

**Managed for daily operations. Break-fix only for one-off projects when you already have an in-house IT lead.**

THE FULL-TIME IT LEAD QUESTION

# Should you just hire in-house?

For aerospace shops under ~200 employees, an internal IT department rarely pencils out. Here's why — and what to do instead.

**One person can't know everything.** Modern aerospace IT spans help desk, network engineering, system administration, cybersecurity, and the specific systems you run — Quantum Control, Pentagon 2000, eMRO, AvSight, Trax, ILS/PartsBase integrations, EDI with primes. Hiring one person and expecting them to do it all is a bad plan.

**Skilled IT hires are hard to find.** The IT skills shortage is real. If you're not technical, you can't reliably interview senior network engineers or evaluate a CISO candidate. You'll spend months and end up with a generalist when you needed three specialists.

**Coverage falls apart.** Everyone gets sick, takes vacation, has emergencies. When your one IT person is out and an AOG ticket comes in at 11 p.m. on a Sunday, who answers?

Internal IT typically makes sense at ~350 employees. Below that, co-managed (your IT lead plus an outsourced firm) usually wins.

THE MATH

## Why internal IT rarely pencils out.

$

**SALARY COSTS**
Senior network engineer: $110–160K. CISO: $180K+. Help desk: $55–75K.

**COVERAGE GAPS**
One person can't cover 24/7 AOG response.

**SINGLE POINT OF FAILURE**
When they leave, knowledge walks out the door.

**SKILL BREADTH**
Network, security, cloud, ERP, compliance — too much for one role.

RECOMMENDATION

**Most aerospace shops under 350 employees are better served by managed or co-managed IT than full-time hires.**

WHY AEROSPACE IS NOW A TOP TARGET

# The threat groups already know your repair-order system.

It's not paranoia. Threat groups are now systematically targeting aviation MROs, parts distributors, and Tier-2 suppliers — and the reasons are simple.

The aerospace supply chain has become one of the most attractive targets in cybercrime. **The data is valuable, the operational pressure to pay ransom is enormous, and the supply-chain leverage gives attackers a path into far bigger fish.**

Major OEMs and primes have spent the last decade hardening their networks. Threat actors have shifted focus downstream — to Tier-2 and Tier-3 suppliers, MROs, and the regional repair stations that keep commercial fleets flying.

For a Part 145 station with a 24/7 AOG desk, every hour of downtime is dollars. **Aircraft sitting on a ramp burn $10,000+ per hour.** The IT defense most aerospace shops have was designed for a 2015 threat model — and 2015 is not what's coming through the door in 2025.

FIVE REASONS

## Why threat actors target aerospace.

**01 VALUABLE DATA**
OEM IP and controlled technical data are worth millions on grey markets.

**02 AOG PRESSURE**
You can't ground a fleet for a week. Ransoms get paid fast.

**03 SUPPLY-CHAIN LEVERAGE**
Lateral access into primes makes you a launch pad.

**04 REGULATED RECORDS**
FAA records, ITAR data, 8130-3 forms — irreplaceable.

BOTTOM LINE

**Aerospace is squarely in the crosshairs. Your IT defense has to match the threat.**

INDUSTRY PRICING BENCHMARKS

# What it actually costs.

RRG managed services are priced per device at a flat monthly rate: **$300/month per server, $150/month per PC or workstation, and $5/month per mobile device** under MDM. No hidden fees, no per-incident charges, no overtime surprises for AOG calls.

## RRG MANAGED IT — MONTHLY PRICING

Per-device flat rate. No hidden fees. Aerospace operators with 24/7 AOG needs sit at the higher end.

| $300 /month | $150 /month | $5 /month |
|---|---|---|
| **PER SERVER** | **PER PC / WORKSTATION** | **PER MOBILE DEVICE** |
| ERP hosts, domain controllers, file servers, backup servers | Desktops and laptops — all employees | Company phones and tablets under MDM management |

### WHAT SHOULD BE INCLUDED

Security patches weekly. Antivirus and firewall monitoring. Backup test restores. Spam filtering. Workstation/server health monitoring. Network documentation.

### WHAT'S OFTEN NOT INCLUDED

Hardware. Software licenses. Special projects (ERP migrations, ITAR enclaves). After-hours/AOG support. Ransomware recovery. Cybersecurity services (priced separately). Get all of this in writing.

GET IN WRITING

**Recovery from a serious cyber-attack can take hundreds of hours. Confirm IN WRITING who pays for that — you, or them.**

CUSTOMER SERVICE · Q1–Q5

# Get the answers in writing.

How an IT firm handles support requests, tickets, and after-hours calls determines what your day looks like at 11 p.m. when an AOG comes in.

**Q1** **When I have an IT problem, how do I get support?**

You should be able to **call, email, or submit a ticket.** If they force you to log in to a portal as the only option, you'll regret it the first time a hangar tech needs help fast. We make it easy: any of the three works.

**Q2** **Do you offer after-hours support? What's the response time?**

Aerospace doesn't run 9-to-5. Our office hours are 9 a.m.–5:30 p.m., and we offer **after-hours emergency support for AOG-impacting outages.** Ask whether after-hours coverage is included in your monthly fee or billed separately — and get the response time commitment in writing.

**Q3** **Do you have a written, guaranteed response time?**

If they don't have it in writing, they can't guarantee it. **Get response time commitments in writing** — both for business hours and after-hours emergency calls.

**Q4** **Will I have a dedicated account manager?**

Smaller firms often can't offer this. Without one, you'll spend time re-explaining your environment to whoever picks up. Our clients get a **dedicated account manager** who knows your stack — your ERP, your repair-order system, your prime-customer EDI feeds.

IT MAINTENANCE · Q6–Q12

# What's actually in the contract.

"All-you-can-eat" managed services contracts almost never are. Every aerospace owner needs to know what triggers an extra invoice — before signing.

**Q6** **Do you offer true managed services with proactive monitoring?**

If they don't watch your network constantly for developing problems, walk away. We catch failing drives on your ERP server before a shift's worth of work orders disappears.

**Q7** **What's NOT included? Specifically: if I get ransomwared, who pays for recovery?**

Recovery from a serious attack can be hundreds of hours. **Get this in writing.** Also confirm: unlimited help desk, M365/Workspace support, line-of-business app support, on-site, multi-site coverage, and disaster rebuilds.

**Q8** **Is your help desk local or outsourced?**

Ask where the help desk is staffed. **Offshore desks accessing systems with controlled technical data can be an ITAR/EAR exposure.** Know who has access to your systems and from where.

**Q9** **How many engineers are on staff?**

One- or two-person firms can't cover a tech being out. We have a full team of certified engineers, including Fortinet-certified network specialists. Coverage doesn't disappear when one person is on PTO.

**Q10** **Do you document our network?**

Yes — at no extra charge, updated quarterly. Documentation protects you, accelerates resolution, and serves as audit evidence for prime-customer and compliance reviews.

**Q11** **Do you meet quarterly for a technology review?**

We do. C-level conversations about your business goals, IT budget, critical projects, compliance obligations, and known risks. Not a geek-fest.

**Q12** **How do I cancel if it isn't working?**

We start every new client with a **3-month trial period.** If you're not satisfied at any point during those 90 days, you can walk away — no penalties, no fines. After that, our agreements are straightforward with no hostage clauses. Our 97% retention is earned, not enforced.

CYBERSECURITY · Q13–Q17

# Your IT firm's defense posture.

What certifications does the firm hold, how do they lock down endpoints, what insurance protects you, and who audits THEIR security? Five questions that separate the real from the rest.

**Q13** **What cybersecurity certifications does your team hold?**

Our engineers are Fortinet-certified and trained against ISO/IEC 27001, NIST 800-171, PCI DSS, and HIPAA. For aerospace clients, that means the **access controls needed to keep ITAR-controlled data segregated and auditable.**

**Q14** **How do you lock down our endpoints?**

Effective security is layered: **MFA on every account, EDR/MDR (not legacy AV), SIEM logging, SOC monitoring, perimeter firewalls with active threat feeds, conditional access, and DLP on controlled technical data.** Don't accept "we have antivirus" as an answer.

**Q15** **What cyber liability and E&O insurance do you carry?**

If their negligence gets you ransomwared, who pays for the lost AOG SLA, the missed turn-times, the operational hit? **RRG is fully insured** — cyber liability, E&O, and workers' comp. Ask to see the policy.

**Q16** **Who audits YOUR cybersecurity?**

Nobody should proofread their own work. We're audited recurringly by Galactic Advisors. If a firm tells you their peers audit them — that's not an audit.

BACKUPS & DISASTER RECOVERY · Q18–Q21

# The day after the disaster.

Hurricanes happen in South Florida. Ransomware happens everywhere. The question is what your shop looks like 24 hours after — and whether your IT firm can actually rebuild what they say they can.

THE QUESTION EVERY OWNER SHOULD ASK

**"When was the last time you tested your backups by restoring them, to see if they actually work?"**

### Q18 How long until my network is back up after a disaster?

Two phases: **fail-over (cloud backup goes live so the team keeps working) and fail-back (restore to the on-prem network).** Critical operations should fail over immediately. Full restoration: 6–8 hours or less. For shops with active AOG obligations, that bar typically tightens further.

### Q19 Do you do periodic test restores of my backups?

Yes — monthly randomized fire drills. **The worst time to "test" a backup is when you desperately need it.** Quick test you can run yourself: copy three files to a thumb drive, delete them from the server, call your IT firm and ask for them back. If they can't do it quickly, you have a problem to fix immediately.

### Q20 If a hurricane hit, how would you keep us operating?

South Florida is in the Atlantic corridor. Multi-day power and internet outages are part of operating reality. **Ask how their existing clients fared during recent hurricanes** — and ask to talk to a couple of them.

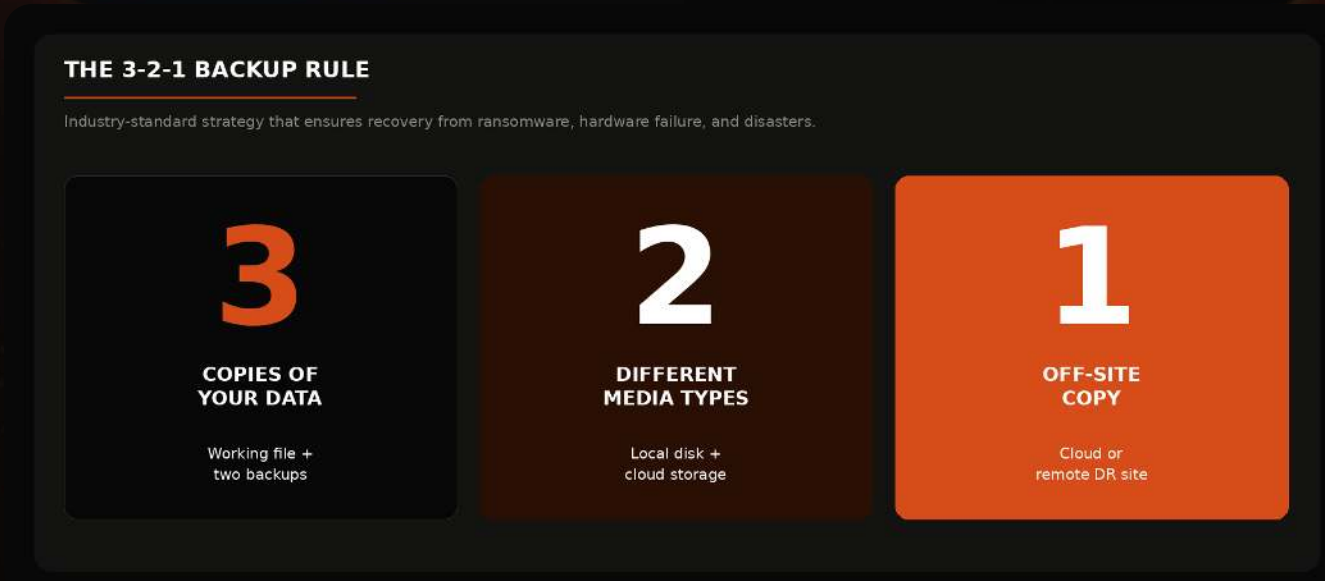
### Q21 Show me your onboarding process.

A real firm has a documented process. Ask for it in writing. Pay attention to how they handle takeover from a hostile predecessor — clean credential rotation, secure data transfer, confirmation that no offboarded accounts retain access.

HOW RECOVERY ACTUALLY WORKS

# The 6-hour rule, and the 3-2-1 strategy.


For aerospace records subject to long FAA retention requirements — and for ITAR-controlled data with separate compliance obligations — **we extend the standard 3-2-1 model with additional off-site copies.**



YOUR NEXT STEP

# A 100% remote, 100% free assessment.

Call our office and reference this guide for a brief 10–15 minute consultation. If we're a fit, we'll schedule our proprietary IT Systems Assessment — conducted entirely remotely, with or without your current IT company knowing.

## AFTER OUR FREE ASSESSMENT, YOU'LL KNOW:

| WHERE YOU'RE OVERPAYING | WHERE YOU'RE EXPOSED | IF BACKUPS WILL ACTUALLY WORK | WHERE YOU'RE OUT OF ALIGNMENT | HOW TO LOWER IT COSTS |
|---|---|---|---|---|
| Or being underserved | Hackers, ransomware, blind spots | FAA-required records | ITAR, NIST 800-171, frameworks | Improve security and uptime |

CALL TODAY

## (844) 919-8534

*Reference this guide for your free assessment. rrgnetworks.com*

FROM ACTIVE ACCOUNTS

# What our clients actually say.

*RRG Networks has greatly helped our network become stable, increase productivity, and decrease expenses. The monthly reports hold great value to really foresee expenses and security flaws we had in our network — allowing a clear path for improvement.*

**Mahesh Raolji**
CEO · JALARAM PRODUCE INC.

*Most importantly, the quick response to our service calls. They always follow through and follow up — an attribute that is distinguishable. We decided to use RRG because of referrals from other companies. They live up to their reputation.*

**Jose Gonzalez**
BRANCH CO · MASSAGE ENVY

*Their attention to detail was very precise and appreciated. After minimal time with the help of RRG, we felt very comfortable with the shift. Their patience and quickness with their responses completely met our needs.*

**Ingrid Gomez**
COMPLIANCE OFFICER · EL AGUILA ENVIOS

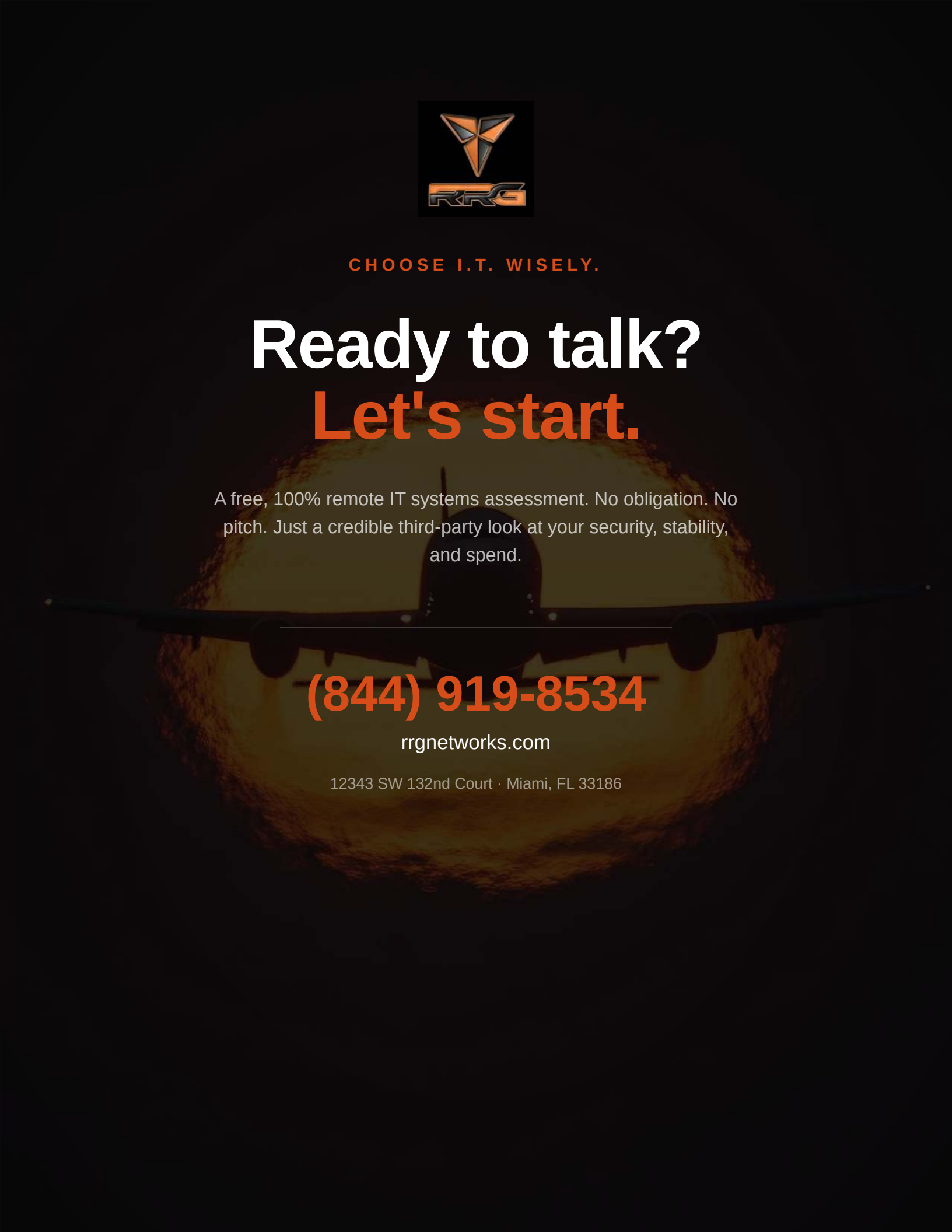
WHY OUR CLIENTS STAY

# Top 7 reasons to outsource to us.

**OUR RESPONSE-TIME PROMISE**

| 9-5:30 | 24/7 | EMERG. | 100% |
|---|---|---|---|
| OFFICE HOURS MON-FRI | SOC SECURITY ALL HOURS | AFTER-HOURS AVAILABLE | NO-SMALL-PRINT GUARANTEE |

1. **Fast response, business hours.**
   Office open 9 a.m.–5:30 p.m. After-hours emergency support available for critical outages.
2. **No geek-speak.**
   You get answers in plain English. We don't talk down to you.
3. **100% no-small-print satisfaction guarantee.**
   If you aren't happy, we make it right. If we can't, the service is free.
4. **Projects on time, on budget.**
   No nickel-and-diming. ERP migrations, ITAR enclaves, network overhauls — what we promised.
5. **No vendor hostage.**
   Full network documentation, written and updated. You can switch firms anytime.
6. **24/7 security monitoring from our SOC.**
   Your network is watched around the clock for threats. Most issues caught and resolved before you notice.
7. **10+ years, 97% client retention.**
   A decade of serving South Florida businesses. Our clients stay because we earn it monthly.



CHOOSE I.T. WISELY.

# Ready to talk?
# Let's start.

A free, 100% remote IT systems assessment. No obligation. No pitch. Just a credible third-party look at your security, stability, and spend.

---

## (844) 919-8534

rrgnetworks.com

12343 SW 132nd Court · Miami, FL 33186