FREEZE FRAME SOLUTIONS

A PLAIN-ENGLISH FIELD GUIDE

The Anchorage IT Buyer's Guide

How managed-IT pricing really works, the contract clauses that bite, the twelve questions to ask before you sign, and a scorecard to grade where your business stands today.

> Your customers see one tenth of your business. Everything in this guide is about the nine tenths underneath it: the systems that have to hold whether or not anyone ever notices them.

ORION GRIMM · FREEZE FRAME SOLUTIONS · ANCHORAGE, ALASKA · FREEZEFRAMESOLUTIONS.COM · (907) 602-1363

SECTION 1

The three ways MSPs charge

Every managed-IT proposal in Alaska is one of three models wearing different fonts. Knowing which one you are reading tells you where the incentives point.

1 · Hourly / break-fix

You pay when something breaks. Sounds thrifty, and for a two-person office with almost no systems it can be. But notice the incentive: the provider earns more when your systems fail more. Nobody on that model is staying late to make sure you never call again. It also makes budgeting impossible; a bad month is an invoice you didn't plan.

2 · Per-user, flat monthly

A fixed price for each employee, everything included. Predictable, easy to compare, and honest in spirit. The catch is the averaging: a user with one laptop pays the same as a user with a workstation, two monitors, a fleet tablet, and a phone. Businesses with complex device footprints quietly subsidize the simple ones, or the "all-inclusive" list grows exclusions in the fine print.

3 · Per-device, flat monthly

A fixed price for each managed device: workstations, servers, network gear. The bill scales with what actually generates work. Add a device, the price moves; retire one, it drops. It requires the provider to keep an accurate inventory, which, conveniently, is also the first thing good security requires.

The question underneath all three

Whatever the model, ask: **"What makes your invoice go up, and can I see that number before it does?"** A trustworthy answer names a unit (a device, a user, a project quote approved in writing). An untrustworthy answer involves the word "depends" and no paper.

Full disclosure of our own bias: Freeze Frame bills per device, flat and monthly, with support hours included, and projects quoted fixed before they start. We think it is the honest model. But any of the three, disclosed clearly and in writing, beats a vague one.

SECTION 2

Contract clauses to watch for

Most MSP contracts are fine until the day you need to leave, have an emergency, or hit renewal. These are the clauses that decide how those days go.

THE CLAUSE	WHAT TO LOOK FOR
Auto-renewal + escalator	Contracts that renew for a full year automatically, with a built-in percentage increase, unless you object inside a narrow window. Fine if disclosed; predatory if buried. Ask: "What happens on month 13, exactly?"
The offboarding clause	The single most important paragraph. Who owns the Microsoft 365 tenant, the domain, the firewall logins, the documentation? What do they hand over, in what format, and is there a "transition fee"? If leaving is expensive and slow, staying was never a choice.
Emergency-rate carve-outs	"Unlimited support" that turns into time-and-a-half after 5pm and double on weekends. Outages don't schedule themselves inside business hours. Get after-hours treatment in writing.
The exclusions appendix	All-you-can-eat plans with an appendix of things that aren't included: servers, "legacy" software, anything called a project. The appendix, not the headline, is the actual contract.
SLAs without teeth	"Target response times" are a goal; an SLA has a remedy. If the contract states response times but no consequence for missing them, it's marketing that made it into a PDF.
Credential custody	Admin passwords held "for security reasons" that you may not view. You can delegate the work of administration. Never delegate away ownership. You should be able to lock *them* out, not the reverse.
Hardware markup opacity	Providers that resell hardware without stating a margin, or that only quote gear paying them the best commission. A fair provider will quote their price, disclose the margin, and tell you when buying it yourself is smarter.

The one-sentence test: ask the provider to explain, out loud, how you would leave them. A good MSP answers calmly and specifically, because they keep clients with good work. Anyone who bristles at the question just answered it.

SECTION 3

Twelve questions to ask before signing

Bring these to the sales meeting. None are hostile; all are revealing. The point isn't the answer alone, it's whether the answer is specific and lands in writing.

01 Who, exactly, answers when we call?

A named person or local team, or a national queue? "Tier 1 offshore triage" is an answer; make sure it's one you're choosing on purpose.

02 What makes the invoice change?

The unit of billing, named. Per device, per user, per hour, and what event moves the number.

03 What happens after hours and on weekends?

Response expectation and rate, both in writing. Outages don't keep office hours in Alaska.

04 What EDR runs on our machines, and who watches it?

A modern answer names a product and a monitoring arrangement. "We install antivirus" is a 2018 answer.

05 When did you last test-restore a client backup?

Not "do you take backups". A date, a duration, a result. Backups that have never been restored are a hope, not a plan.

06 Do you support both Microsoft 365 and Google Workspace?

If they only run one, every recommendation you ever get will point there, whatever fits your team.

Questions seven through twelve

07 **What do we own, and what do you hold?**

Tenant, domain, licenses, admin credentials, documentation. The answer should be "you own all of it."

08 **How do we leave you?**

The offboarding process, the timeline, and the cost, described before you've signed anything.

09 **How are projects priced?**

Fixed-scope quotes approved before work starts, or hours discovered at month-end? One of these produces budget surprises.

10 **What's your onboarding, and what does it cost?**

A real onboarding (inventory, documentation, security baseline) takes weeks and should be described concretely. Watch for setup fees that appear later.

11 **Can we see a sample monthly report?**

You're buying invisible work. The report is how you see it: patching, incidents, backups verified, licenses. No report means no visibility.

12 **Which of your clients can we call?**

References from businesses your size, in Alaska. Distance-support from the Lower 48 feels different in week three than in the sales meeting.

SECTION 4

The IT maturity scorecard

Grade yourself honestly: one point per box you can check *with evidence*, not from memory. This is the same ground our free 30-minute IT Health Check covers in person.

Identity & access / 4

- ☐ MFA enforced for every user, with legacy sign-in protocols disabled
- ☐ Admin accounts separate from daily-driver accounts
- ☐ Departed employees disabled the day they leave (check the last three)
- ☐ Someone reviews who-has-access-to-what at least twice a year

Endpoints / 3

- ☐ Modern EDR on every computer, monitored by a human arrangement, not just installed
- ☐ Disks encrypted (BitLocker / FileVault) on every laptop that leaves the building
- ☐ Operating systems and third-party apps patched on a schedule you could describe

Backup & recovery / 3

- ☐ Backups exist for everything you'd cry about, including cloud data
- ☐ At least one copy is separated from your network and credentials
- ☐ A test restore has succeeded in the last six months, and someone wrote it down

Network / 3

- ☐ Guest Wi-Fi fully isolated from business systems
- ☐ Firewall firmware current; default passwords long gone
- ☐ You know every device on the network (an inventory exists and is current)

Paper & people / 3

- ☐ A written incident-response plan reachable when systems are down
- ☐ Cyber-insurance application answers verified against reality, not aspiration
- ☐ Documentation (configs, licenses, vendors) lives somewhere your business owns

What your score means

0 – 6 · Exposed

One bad click or one failed drive is currently a business-threatening event. Start with MFA, EDR, and a separated backup, in that order.

7 – 11 · Foundations

The bones exist but the proof doesn't. Close the gaps and, above all, start writing things down; undocumented controls fail audits and claims.

12 – 16 · Defensible

You're ahead of most small businesses. The remaining work is drift: keeping this true every quarter, not just today.

Want this scored for you, for free?

The Freeze Frame **30-minute IT Health Check** walks this exact ground against your real environment: five findings, in writing, no obligation and no sales pitch. You keep the report either way.

(907) 602-1363 · freezeframesolutions.com/free-assessment · Anchorage & the Mat-Su Valley