

Managed IT Services Proposal

Prepared for **Larkspur Accounting Group**, 14 Orchard Lane, Suite 300, Springfield

Prepared by **Northbeam IT Services**

Proposal date: October 6, 2026. This proposal is valid until November 30, 2026.

Proposal reference: NB-2026-1147

Contents

1. Executive summary
2. About Northbeam
3. Your current environment
4. Our approach
5. Scope of services
6. Help desk and support hours
7. Security services
8. Backup and disaster recovery
9. Service levels and response times
10. Onboarding plan
11. Team and contacts
12. Pricing summary
13. One-time fees
14. What is not included
15. Price changes
16. Term and renewal
17. Ending the agreement
18. Data handling and privacy
19. Customer responsibilities
20. Reporting and reviews
21. Insurance and liability
22. Acceptance

1. Executive summary

Larkspur Accounting Group asked us to propose a fully managed IT service for its office of 24 staff during the busy tax season and the rest of the year. This proposal covers help desk support, device monitoring, security, backups and planning.

In short, we recommend our Professional plan for all 24 users at a fixed monthly fee, with a one-time onboarding project to bring every device and account up to our standard. Details on price, term and renewal are in sections 12 to 17, and we encourage you to read them closely.

Our goal is simple: when someone at Larkspur has a computer problem, they make one call and it gets fixed, and the partners never have to think about backups or security again.

Our clients tell us that the biggest change after moving to managed IT is predictability: a known monthly cost, known response times and a written plan for what happens when things go wrong.

2. About Northbeam

Northbeam IT Services has supported professional services firms since 2011. We look after about 140 small and mid-sized offices, most of them accounting, legal and insurance practices with between 10 and 80 staff.

Our team works from two offices and includes help desk technicians, systems engineers and a dedicated security analyst. Every client has a named account manager who meets with them on a regular schedule.

We focus on keeping day-to-day IT quiet so that your staff can focus on client work. That means fewer surprises, clear documentation and a single number to call when something breaks.

Our clients tell us that the biggest change after moving to managed IT is predictability: a known monthly cost, known response times and a written plan for what happens when things go wrong.

Northbeam IT Services has supported professional services firms since 2011. We look after about 140 small and mid-sized offices, most of them accounting, legal and insurance practices with between 10 and 80 staff.

Our team works from two offices and includes help desk technicians, systems engineers and a dedicated security analyst. Every client has a named account manager who meets with them on a regular schedule.

3. Your current environment

During our site visit on September 22, 2026, we reviewed the office network, the 24 staff laptops, the two shared printers, the file server and the Microsoft 365 tenant.

Most laptops are between two and five years old. Six of them are running an operating system version that will stop receiving security updates next year and should be replaced or upgraded.

The file server is backed up to a USB drive that is taken home on Fridays. This works, but it depends on one person remembering, and a restore has not been tested in over a year.

Multi-factor sign-in is turned on for partners but not yet for all staff. Email filtering is the default level that comes with the subscription.

The office firewall is in good condition and its support contract runs until March 2028. The wireless network uses a single shared password for staff and guests.

Item	Count	Notes
Staff laptops	24	Six need replacement or upgrade
Shared printers	2	Under a separate lease
File server	1	USB backup, taken home weekly
Firewall	1	Supported until March 2028
Microsoft 365 users	24	Multi-factor sign-in for partners only

4. Our approach

We start with a stabilize phase: document everything, fix the urgent risks and bring every device under monitoring.

Next comes a standardize phase, where we bring laptops, accounts and settings to one consistent setup so problems are easier to prevent and faster to fix.

Finally we move into an improve phase with quarterly reviews, a rolling hardware plan and a yearly security check.

Throughout all three phases, your staff contact the help desk the same way, by phone, email or the client portal.

During our site visit on September 22, 2026, we reviewed the office network, the 24 staff laptops, the two shared printers, the file server and the Microsoft 365 tenant.

Most laptops are between two and five years old. Six of them are running an operating system version that will stop receiving security updates next year and should be replaced or upgraded.

5. Scope of services

The Professional plan includes the services below for every covered user and device.

Service	Included
Unlimited remote help desk during support hours	Yes
24/7 device monitoring and alerts	Yes
Operating system and app patching	Yes
Microsoft 365 account management	Yes
Antivirus and endpoint protection	Yes
Email filtering, advanced level	Yes
Daily cloud backup of the file server	Yes
Quarterly business review	Yes
On-site visits	Up to 2 per month

Anything not listed here, or listed in section 14, is outside the scope of this proposal and would be quoted separately.

6. Help desk and support hours

Our help desk is staffed from 7:00 am to 6:00 pm, Monday to Friday, excluding public holidays. During these hours all remote support is included in your monthly fee.

Support outside these hours is billed at \$185 per hour, with a one-hour minimum. This includes evenings, weekends and public holidays. Many accounting clients use after-hours support during tax season, so please plan for this.

You can reach the help desk by phone, by email or through the client portal. Every request gets a ticket number so you can follow its progress.

Throughout all three phases, your staff contact the help desk the same way, by phone, email or the client portal.

7. Security services

Security is part of every plan. We turn on multi-factor sign-in for every user, roll out endpoint protection to every laptop and set email filtering to the advanced level.

Each quarter we send a short phishing test to staff and share the results with the partners. Staff who click a test link get a five-minute training video.

Our security analyst reviews alerts every business day. Urgent alerts at night or on weekends page our on-call engineer.

Multi-factor sign-in is turned on for partners but not yet for all staff. Email filtering is the default level that comes with the subscription.

The office firewall is in good condition and its support contract runs until March 2028. The wireless network uses a single shared password for staff and guests.

8. Backup and disaster recovery

We replace the USB drive backup with a daily cloud backup of the file server and of every Microsoft 365 mailbox and OneDrive.

Backups are kept for 30 days. Longer retention, for example seven years for client tax files, is available as an add-on and is not included in the price in section 12.

We test a restore every quarter and send you the result. If the office cannot be used, our goal is to have staff working again from their laptops within one business day.

We start with a stabilize phase: document everything, fix the urgent risks and bring every device under monitoring.

9. Service levels and response times

Response time is how long it takes us to start working on a request, not how long it takes to fix it.

Priority	Example	Response time
Critical	Whole office cannot work	1 hour
High	One person cannot work	4 business hours
Normal	Something is slow or annoying	Next business day
Low	Questions and small changes	Within 3 business days

If we miss a Critical response time more than twice in one calendar month, you receive a credit of 5% of that month's fee. This is the only credit offered for missed service levels.

10. Onboarding plan

Onboarding takes about six weeks. Week 1 is discovery and documentation. Weeks 2 and 3 roll out monitoring, endpoint protection and multi-factor sign-in. Weeks 4 and 5 move backups to the cloud and test a restore. Week 6 is a review with the partners.

We recommend starting onboarding no later than mid-December so the office is stable before tax season.

We start with a stabilize phase: document everything, fix the urgent risks and bring every device under monitoring.

Next comes a standardize phase, where we bring laptops, accounts and settings to one consistent setup so problems are easier to prevent and faster to fix.

Finally we move into an improve phase with quarterly reviews, a rolling hardware plan and a yearly security check.

11. Team and contacts

Your account manager will be Dana Ruiz. Your lead engineer will be Sam Okafor. The help desk can be reached at the number on the client portal.

Escalations go first to the lead engineer, then to the account manager, then to our operations director.

Our team works from two offices and includes help desk technicians, systems engineers and a dedicated security analyst. Every client has a named account manager who meets with them on a regular schedule.

We focus on keeping day-to-day IT quiet so that your staff can focus on client work. That means fewer surprises, clear documentation and a single number to call when something breaks.

12. Pricing summary

Item	Price
Professional plan, per user per month	\$143.75
Users covered	24
Monthly fee	\$3,450.00
Billing	Monthly in advance
Minimum term	36 months

The monthly fee covers all services in section 5 for 24 users. Adding a user adds \$143.75 per month. Removing users can only lower the monthly fee by up to 10% during the term.

Prices do not include sales tax.

13. One-time fees

A one-time onboarding fee of \$4,800 is due when the agreement is signed. It covers the work described in section 10.

Replacing the six older laptops is not included. We can quote hardware separately, or you can buy it yourself and we will set it up at no extra charge.

Most laptops are between two and five years old. Six of them are running an operating system version that will stop receiving security updates next year and should be replaced or upgraded.

14. What is not included

The following are not included in the monthly fee and are billed separately when needed:

- Software licenses, including Microsoft 365 and tax software subscriptions
- Printer repairs and printer supplies (these are covered by your printer lease)
- Hardware and replacement parts
- Work outside support hours (see section 6)
- Projects such as office moves or new phone systems
- Backup retention beyond 30 days (see section 8)

15. Price changes

We may increase the monthly fee by up to 6% once every 12 months during the term, with 30 days written notice. Increases reflect changes in our labor and software costs.

We will not change the per-user price during the first 12 months of the agreement.

Our clients tell us that the biggest change after moving to managed IT is predictability: a known monthly cost, known response times and a written plan for what happens when things go wrong.

16. Term and renewal

The agreement starts on the date onboarding begins and runs for an initial term of 36 months.

At the end of the initial term, the agreement renews automatically for another 36 months unless either party gives written notice at least 90 days before the end of the term.

Renewal terms use the monthly fee in effect at the time of renewal, including any increases under section 15.

Finally we move into an improve phase with quarterly reviews, a rolling hardware plan and a yearly security check.

17. Ending the agreement

Either party may end the agreement for a serious breach that is not fixed within 30 days of written notice.

If you end the agreement early for any other reason, an early termination fee equal to 75% of the monthly fees remaining in the current term is due.

When the agreement ends, we hand over all documentation, passwords and backups within 10 business days. Help moving to a new provider is billed at our standard project rate.

18. Data handling and privacy

Client data stays in data centers in the United States. Our staff only access your systems to deliver the services in this proposal.

We follow a written security policy and our staff complete yearly privacy training. We will tell you within 72 hours if we learn of a security incident that affects your data.

The file server is backed up to a USB drive that is taken home on Fridays. This works, but it depends on one person remembering, and a restore has not been tested in over a year.

19. Customer responsibilities

To deliver these services, we need a named office contact, remote access to all covered devices, and notice of new staff at least three business days before their start date.

Staff should report problems through the help desk rather than contacting engineers directly, so every request is tracked.

Throughout all three phases, your staff contact the help desk the same way, by phone, email or the client portal.

20. Reporting and reviews

Every month you receive a one-page report showing tickets opened and closed, response times, backup status and security alerts.

Every quarter, your account manager meets with the partners to review the report, plan upcoming hardware replacements and discuss any changes to the office.

Finally we move into an improve phase with quarterly reviews, a rolling hardware plan and a yearly security check.

21. Insurance and liability

We carry general liability and cyber liability insurance and can provide certificates on request.

Our total liability under the agreement is limited to the fees you paid in the 6 months before the claim.

Northbeam IT Services has supported professional services firms since 2011. We look after about 140 small and mid-sized offices, most of them accounting, legal and insurance practices with between 10 and 80 staff.

22. Acceptance

To accept this proposal, sign below and return it before November 30, 2026. Onboarding will be scheduled within 10 business days of signing.

For Larkspur Accounting Group: _____ Date: _____

For Northbeam IT Services: _____ Date: _____

Appendix A: Glossary

Endpoint protection: Software on each laptop that blocks and reports threats.

Multi-factor sign-in: A second check, like a code on your phone, when you sign in.

Patching: Installing updates that fix bugs and security holes.

Response time: How quickly we start working on a request.

Retention: How long backup copies are kept.