PHANTOM GUARDIAN MSA — CLIENT SUMMARY (PLAIN LANGUAGE)

Phantom Technology Solutions, LLC

Aligned to MSA Version 3.1 | Updated September 28, 2026

UNDERSTANDING YOUR AGREEMENT WITH PHANTOM TECHNOLOGY SOLUTIONS

PLAIN LANGUAGE SUMMARY — NOT A LEGAL DOCUMENT. This summary is provided for your convenience. It does not replace your Master Services Agreement or Statement of Work. In the event of any conflict, the executed SOW and incorporated MSA govern.

1. YOUR AGREEMENT DOCUMENTS

You only need to sign **ONE document**: your Statement of Work (SOW). The Master Services Agreement (MSA) is incorporated into your SOW by reference — by signing the SOW, you are automatically agreeing to all MSA terms. You do not need to separately sign the MSA.

The MSA is available to read at any time at: https://www.phantomts.com/legal/msa

Legal notices to PTS: Attn: Legal Notices, 5097 N 600 E, Rolling Prairie, IN 46371; copy legal@phantomts.com. Follow MSA Section 18.2 for notice delivery and receipt.

What this means for you: Review the MSA before signing your SOW. Once you sign the SOW, you are bound by both documents. Keep both your signed SOW and the incorporated MSA version, together with any required signed addenda.

The MSA is a comprehensive, self-contained document. All program definitions, service terms, compliance requirements, and governance provisions are built into the MSA body. Here is where to find key topics:

- Guardian Tier Definitions and Service Alignment — Section 3B of the MSA
- Residential Terms — Section 4B of the MSA
- Acceptable Use Policy (AUP) — Section 5B of the MSA
- Security Baseline Requirements and Policies — Section 5C of the MSA
- Service Level Targets and Support Terms — Section 6B of the MSA
- Onboarding and Offboarding Procedures — Section 7 of the MSA
- Change Management — Section 8 of the MSA

- Incident Response Scope and Fees — Section 9B of the MSA
- Data Protection Terms — Section 10B of the MSA
- Healthcare and HIPAA Services — Section 10C of the MSA
- Third-Party Services — Section 11B of the MSA
- AI Services — Section 11C of the MSA
- Fees and Payment (Pricing Framework) — Section 12 of the MSA
- Liability Cap Matrix — Section 16.2 of the MSA

Your SOW identifies which Guardian tier you are in. Your tier determines the scope of services, the level of PTS accountability, and which terms within the MSA apply to your engagement.

What this means for you: You sign one document — your SOW (which incorporates the MSA by reference). The core service terms are in the MSA. A separate BAA, Shared Responsibility Matrix, or other addendum may also be required. Keep the complete agreement package on file.

2. YOUR GUARDIAN TIER

PTS offers five service tiers. Your SOW identifies which tier applies to you:

Guardian Ad-Hoc

Reactive, on-demand support. No ongoing monitoring, no managed security, no SLA. You call us when you need help, and we bill by the hour. You are responsible for your own IT environment.

What this means for you: We are available when you need us, but we are not watching your systems between calls. If something goes wrong, you notify us.

Guardian Residential

For personal and household use only. We manage and secure your home devices, home network, and family technology. This tier includes endpoint protection, cloud backup, password management, and priority remote support during business hours. This is not for business or regulated use — if you start using any covered device for commercial work, let us know immediately. Residential terms are governed by Section 4B of the MSA.

What this means for you: Think of us as your family's personal IT team. We keep your home network and devices secure so you don't have to.

Guardian Fundamentals

We are your IT department. We manage your endpoints, Microsoft 365, patching, EDR and MDR/SOC, backup, and network monitoring. Remote and on-site helpdesk support is provided within the SOW allowance, with no travel charges within the stated service area. We handle user onboarding/offboarding (per Section 7 of the MSA) and provide regular technology reviews. Designed for small businesses with no internal IT staff.

What this means for you: You focus on your business. We handle the technology, the security, and the day-to-day IT operations.

Guardian Compliance

Everything in Fundamentals, plus security governance led by a virtual Chief Information Security Officer (vCISO). We conduct risk assessments, develop security policies, run training and phishing simulations, support your cyber insurance requirements, and help you align with regulatory frameworks. Incident response is handled per Section 9B of the MSA (Incident Response Scope and Fees). Designed for businesses that must demonstrate security to regulators, insurers, or clients.

What this means for you: We don't just manage your IT — we help you prove to auditors, insurers, and clients that your security program is real and documented.

Guardian Co-Managed

For organizations that already have an IT team. We provide enterprise-grade security monitoring, managed EDR, firewall management, escalation support, and strategic governance. Change management procedures are governed by Section 8 of the MSA. Your IT team handles day-to-day operations; we handle security and advanced engineering.

What this means for you: We extend and strengthen your existing IT team. We handle the hard security problems so your team can stay focused on operations.

3. WHAT WE DO FOR YOU

The specific services you receive depend on your tier. Here is a simplified overview:

Service	Ad-Hoc	Residential	Fundamentals	Compliance	Co-Managed
Proactive monitoring	—	Home network	✓	✓	✓ (security focus)
Endpoint protection	—	✓ (lite)	✓ (EDR)	✓ (EDR)	✓ (EDR)
Patch management	—	Basic	✓	✓	Coordinated
Backup management	—	Cloud	✓	✓	Per SOW
M365 administration	—	—	✓	✓	Shared
User onboard/offboard	—	Family devices	✓	✓	Client IT executes
Helpdesk support	Hourly	Business hrs	Business hrs	Hours defined in SOW	Client IT (Tier 1)
Security governance	—	—	—	✓ (vCISO)	✓ (optional vCISO)

Risk assessments	—	—	—	✓ (annual)	Per SOW
Compliance advisory	—	—	—	✓	Per SOW
Phishing simulation	—	—	Included per SOW	Monthly or quarterly per SOW	Per SOW
Incident response	—	—	Initial triage/advisory; extended response separate	✓ + report	✓ + coordination

Note: Full service level targets and response time commitments are defined in Section 6B of the MSA (Service Level Targets). Baseline security requirements you must maintain are defined in Section 5C of the MSA (Security Baseline Requirements).

Standard Business Hours are Monday through Friday, 9:00 AM to 5:00 PM Eastern, excluding PTS-observed holidays. Emergency billing, discounts, support allowances, and included service area are specified in your SOW; 24/7 security monitoring is not the same as unlimited 24/7 helpdesk support.

4. WHAT YOU AGREE TO DO

Your agreement works both ways. Here is what we need from you:

- **Give us access** — We need administrative access to the systems we manage. Without it, we cannot do our job.
- **Tell us when things change** — New employees, departing staff, new devices, office moves, new software — let us know so we can keep your environment secure and documented. Change management procedures are in Section 8 of the MSA.
- **Pay on time** — Invoices are due per your SOW terms. Auto-pay is required. Late payments accrue interest. Payment terms are set forth in Section 12 of the MSA.
- Annual price adjustments are governed by MSA Section 12.11: increases shall not exceed the greater of 5% or the applicable CPI-U change, with at least 60 days' written notice. Quarterly and annual prepayment discounts, when elected in the SOW, apply to recurring fees only, not one-time, project, or out-of-scope fees.
- **Maintain your systems** — Keep your operating systems current, maintain your licenses, and meet the baseline requirements in Section 5C of the MSA (Security Baseline Requirements).

- **Use systems appropriately** — Acceptable use of PTS-managed systems is governed by Section 5B of the MSA (Acceptable Use Policy).

5. IF THINGS GO WRONG

If you experience a security incident, technical failure, or service disruption:

What PTS will do

- Respond through approved support channels under the applicable business hours, severity targets, and SOW scope
- Assess and contain the incident within our scope
- Coordinate with your team and relevant third parties
- Provide post-incident reporting at qualifying tiers

What You Must Do

- Cooperate fully with our investigation and response
- Preserve all logs and evidence as instructed
- Do not attempt to resolve the incident independently without coordinating with PTS

What's NOT Included (Unless Separately Contracted)

- Full digital forensic investigation
- Legal notification to regulators, law enforcement, or affected individuals
- Ransom negotiation or ransom payment
- Public relations or media response

What this means for you: In a crisis, call us first. We coordinate the response. Your job is to cooperate fully and preserve evidence. Do not try to fix it yourself — that can make things worse.

6. WHAT WE DON'T PROMISE

No technology provider — no matter how good — can guarantee 100% security. Cyber threats evolve constantly, and even the best defenses can be breached.

PTS significantly reduces your risk through expert management, proactive monitoring, security governance, and industry best practices. But we cannot prevent every possible attack, outage, or data loss event.

We strongly recommend that every client maintain cyber liability insurance appropriate to their tier and risk profile:

- Fundamentals clients: minimum $500,000 in coverage recommended
- Compliance and Co-Managed clients: minimum $1,000,000 in coverage recommended

What this means for you: We significantly reduce your risk — but we cannot eliminate it. Cyber insurance is your financial safety net when things go wrong despite best efforts.

7. YOUR LIABILITY CAP

Your agreement limits PTS's total financial liability. The cap depends on your tier. Full details are available in Section 16.2 of the MSA (Liability Cap Matrix).

Your Tier	Maximum PTS Liability
Ad-Hoc	$5,000 or fees paid for the specific service, whichever is less
Residential	$10,000 or 2 months of recurring fees, whichever is less
Fundamentals	$25,000 or 3 months of recurring fees, whichever is less
Compliance	$75,000 or 6 months of recurring fees, whichever is less
Co-Managed	$75,000 or 6 months of recurring fees, whichever is less

These caps apply when you have met your responsibilities under the agreement (including Section 5C of the MSA — Security Baseline Requirements). If an incident results from actions you controlled (for Co-Managed clients, actions by your internal IT team), the cap may be proportionally reduced.

What this means for you: Our liability is capped. This is standard in managed IT agreements. The cap increases as your tier — and our accountability — increases. Maintain your baseline requirements to preserve your full cap.

8. WHEN WE PART WAYS

Non-renewal generally requires 60 days' notice under Section 13.2. Termination for convenience is a different process: 90 days for commercial clients and 30 days for Residential, with the applicable early-termination fee. Your executed SOW may expressly vary these terms.

- Data return: PTS returns Client Data within 15 business days of termination and destroys remaining copies within 60 days, unless longer retention is required by law. PHI is subject to the BAA and Section 10C, including its separate certification requirement.

- Transition assistance: Section 7.5 provides for up to 30 days of transition assistance while applicable fees continue. Separately scoped or out-of-scope work follows the SOW and Section 12.6; do not assume all transition work is automatically an additional hourly charge.
- **PTS tools removed** — PTS will remove all PTS-deployed agents, tools, and software from your systems. You are responsible for replacing any security or monitoring tools PTS removes.
- **Residential clients: Section 7.7 governs offboarding, together with the household data protections in Section 4B.**

What this means for you: When we part ways, you get your data back and we clean up our tools. Plan ahead — leaving without a replacement security stack puts you at risk.

9. YOUR DATA

PTS only uses your data to deliver the services described in your SOW. We do not sell your data, use it for marketing, or share it except as required to deliver your services. Data protection obligations are governed by Section 10B of the MSA.

Third-party services and subprocessors integrated into your environment are governed by Section 11B of the MSA. Where applicable, AI tools used in the management of your environment are governed by Section 11C of the MSA (AI Services).

Residential clients: Your household and personal data is never used for commercial purposes. PTS treats Residential client data with heightened privacy protections as described in Section 4B of the MSA (Residential Terms).

For healthcare clients: If you are subject to HIPAA, your data handling obligations and Business Associate Agreement terms are addressed in Section 10C of the MSA (Healthcare and HIPAA Services).

What this means for you: Your data is yours. We use it only to deliver your services. We tell you who we share it with, and we are bound by the same data protection obligations we put in writing.

10. MSA SECTION REFERENCE

For your convenience, the following table summarizes all key MSA sections. Everything is integrated into the Master Services Agreement — there are no standalone exhibit files.

MSA Section	Content
Section 3B of the MSA	Guardian Tier Definitions and Service Alignment
Section 4B of the MSA	Residential Terms
Section 5B of the MSA	Acceptable Use Policy (AUP)
Section 5C of the MSA	Security Baseline Requirements and Policies

Section 6B of the MSA	Service Level Targets and Support Terms
Section 7 of the MSA	Onboarding / Offboarding Procedures
Section 8 of the MSA	Change Management
Section 9B of the MSA	Incident Response Scope and Fees
Section 10B of the MSA	Data Protection Terms
Section 10C of the MSA	Healthcare and HIPAA Services
Section 11B of the MSA	Third-Party Services
Section 11C of the MSA	AI Services
Section 12 of the MSA	Fees and Payment (Pricing Framework)
Section 16.2 of the MSA	Liability Cap Matrix

11. DOCUMENT STRUCTURE REFERENCE

The following table summarizes the documents in your agreement. You only need to sign **one document** — your SOW.

Document	Status / Description
Master Services Agreement (MSA)	Reference only — available at https://www.phantomts.com/legal/msa. Incorporated into your SOW by reference. No separate signature required.
Statement of Work (SOW)	Required — Client and PTS sign
Services Catalog	Reference only; overview of Guardian service models, subject to SOW scope
MSA Client Summary	Reference only — no signature required. Plain-language summary for clients.

QUESTIONS?

If you have questions about your agreement, your tier, your services, or anything in this summary, contact us:

Phantom Technology Solutions, LLC

Rolling Prairie, Indiana

(800) 338-4474

support@phantomts.com

IMPORTANT REMINDER: This summary is provided for your convenience. It does not replace your Master Services Agreement or Statement of Work. In the event of any conflict, the executed SOW and incorporated MSA govern.