PHANTOM GUARDIAN — SERVICES CATALOG

Phantom Technology Solutions, LLC

Aligned to MSA Version 3.1 | Updated September 28, 2026

Rolling Prairie, Indiana

IT Management | Cybersecurity | Residential Technology

"We protect what matters — from your home network to your business infrastructure."

For prospective and current clients

SECTION 1: ABOUT PHANTOM TECHNOLOGY SOLUTIONS

Phantom Technology Solutions, LLC (PTS) is an Indiana-based managed services provider headquartered in Rolling Prairie, La Porte County, Indiana. PTS delivers IT management, cybersecurity, and residential technology services under the Phantom Guardian brand.

PTS operates on a Guardian model: we take ownership of what we manage, maintain accountability for the outcomes we control, and clearly define the shared responsibility between PTS and each client.

Our client base ranges from individual households and remote workers to small businesses, regulated professional firms, and mid-size manufacturers with internal IT teams. Regardless of client size, every engagement is built on the same core principles: tiered accountability, transparent scope, and measurable security improvement.

Our Mission

"We protect what matters — from your home network to your business infrastructure."

SECTION 2: THE GUARDIAN FRAMEWORK

Philosophy

The Phantom Guardian framework is built on three principles:

- **Tiered Accountability** — PTS accepts defined levels of ownership and accountability based on the service tier. Higher tiers mean more PTS responsibility.
- **Shared Responsibility** — Every engagement is a partnership. PTS delivers expert services; the client fulfills defined responsibilities. Neither party can succeed alone.
- **Risk-Aligned Services** — Services are designed to match the client's actual risk profile, not a one-size-fits-all checklist. Residential households need different protection than regulated law firms.

> *Key Principle: Guardian services reduce risk — they do not eliminate it. No technology provider can guarantee 100% security. PTS significantly reduces risk through expert management, proactive monitoring, and structured governance. Cyber insurance is always recommended.*

Five-Tier Structure

Tier	Target Client	Core Value Proposition
Guardian Ad-Hoc	Organizations not ready for managed IT	Reactive support without a recurring managed-service commitment; SOW or Order Form required
Guardian Residential	Households, remote workers, executive homes	Home and family technology, secured and supported
Guardian Fundamentals	SMBs with no internal IT (1–50 users)	Your IT department — fully managed, fully accountable
Guardian Compliance	Regulated industries, insurance mandates	Governance, risk, and accountability for compliance-driven businesses
Guardian Co-Managed	Organizations with internal IT staff	Enterprise-grade security for teams that already have IT

SECTION 3: TIER DESCRIPTIONS

Guardian Ad-Hoc

"Reactive support when you need it. No recurring managed-service commitment or ongoing monitoring."

Target Client

Organizations or individuals not ready or willing to commit to a managed IT relationship. Clients who need occasional expert help on a time-and-materials basis.

What's Included

- Time-and-materials support (billed hourly)
- Remote or on-site troubleshooting as requested
- Project-based work (network setup, migrations, etc.)
- No recurring managed-service fees; engagement minimums and labor rates apply under the SOW or Order Form

What's NOT Included

- No proactive monitoring, patching, or security management
- No SLA or guaranteed response times

- No endpoint protection deployment or EDR
- No backup management
- No compliance or governance services
- Not permitted for regulated workloads

Who Owns What

Client retains 100% responsibility for their IT environment. PTS provides expert labor on request only.

Qualification Requirements

Universal baseline obligations apply. Sign an SOW or Order Form incorporating the MSA and authorize each engagement.

Transition Path

When the client needs consistent support, proactive monitoring, or security management, PTS will recommend upgrading to Guardian Residential (households) or Guardian Fundamentals (businesses).

Guardian Residential

"Home and family technology, secured and supported."

Target Client

Households, remote workers, executive home offices, and families who want professional technology management and cybersecurity for their personal devices and home networks.

What's Included

- Personal device management (Windows, Mac, iOS, Android — per SOW scope)
- Home network monitoring and basic security hardening
- Managed endpoint protection (antivirus/EDR lite)
- Cloud backup for personal and family devices
- Password manager setup and ongoing support
- Family device onboarding/offboarding
- Parental controls setup and maintenance (where applicable)

- Phishing awareness and personal cyber hygiene coaching
- Priority business-hours remote support (M–F, 9 AM – 5 PM ET)
- Standard hours exclude PTS-observed holidays; response targets are objectives, not guarantees.
- Annual home tech health review
- New device setup as expressly scoped and priced in the SOW

What's NOT Included

- Business/commercial systems or regulated data (use Fundamentals or higher)
- SLA guarantees equivalent to commercial tiers
- Compliance management
- After-hours emergency support (unless separately contracted)
- On-site visits (unless separately quoted)

Who Owns What

PTS owns security tool deployment, backup management, and proactive monitoring within scope. Client owns maintaining devices on supported OS, reporting issues, and keeping internet connectivity.

Qualification Requirements

- Consistent household device footprint
- Agreement to PTS-approved security tools on all covered devices
- Signed SOW; residential terms governed by Section 4B of the MSA

Transition Path

When the client starts a business, acquires commercial systems, or needs compliance management, PTS will recommend transitioning to Guardian Fundamentals.

Guardian Fundamentals

"Your IT department — fully managed, fully accountable."

Target Client

Small businesses (1–50 users) with no dedicated internal IT staff. Organizations that want a reliable, accountable IT partner to manage their entire technology environment.

What's Included

- Endpoint management and security (managed EDR across all devices)
- Microsoft 365 administration and optimization
- Patch management (OS and application)
- Managed backup and recovery
- Network monitoring and alerting
- User onboarding/offboarding (per Section 7 of the MSA)
- Remote and on-site helpdesk support (M–F, 9 AM – 5 PM ET), within the SOW support allowance; no travel charges within the SOW-defined service area
- Emergency service availability, separate billing, any discounts, and support-pool treatment are expressly stated in the SOW. After-hours service is not implied to be unlimited or included.
- Regular technology reviews and planning
- Managed MDR/SOC, security awareness training, and phishing simulations as scoped in the SOW
- Vendor coordination for technology decisions

What's NOT Included

- Security governance, vCISO, or compliance advisory (upgrade to Compliance)
- Formal risk assessments and compliance-governance programs
- After-hours emergency support (unless separately contracted)
- Regulated workloads without a Compliance overlay

Who Owns What

PTS owns the IT environment management, security tooling, and support delivery. Client owns business decisions, vendor approvals, and employee cooperation with PTS procedures.

Qualification Requirements

- PTS assessment of current environment completed
- Agreement to PTS-standard security toolstack
- Signed SOW; all terms governed by the MSA

Transition Path

When a regulatory requirement emerges, when cyber insurance mandates formal governance, or when the client's risk exposure grows, PTS recommends transitioning to Guardian Compliance.

Guardian Compliance

"Governance, risk, and accountability for compliance-driven businesses."

Target Client

Regulated businesses, licensed professional firms, healthcare organizations, financial services companies, and any client with a cyber insurance mandate requiring formal security governance.

What's Included

Everything in Guardian Fundamentals, plus:

Compliance support hours, including any extended-hours window, must be expressly defined in the SOW.

- Virtual Chief Information Security Officer (vCISO) — quarterly strategic oversight
- Annual formal risk assessment and remediation roadmap
- Security policy development, review, and maintenance
- Annual security awareness training program
- Cyber insurance readiness support
- Regulatory compliance alignment advisory (HIPAA, GLBA, FTC Safeguards, etc.)
- Incident response coordination with post-incident reporting (see Section 9B of the MSA)

- Annual tabletop exercise
- Quarterly cyber posture scorecard
- Compliance roadmap and prioritized remediation planning

What's NOT Included

- Guaranteed regulatory certification or audit outcomes
- Legal, insurance, or formal attestation services
- Clinical, billing, or operational healthcare responsibilities
- Digital forensics beyond initial incident triage (separately contracted)

Who Owns What

PTS owns security governance, risk assessment, policy development, training, and compliance advisory. Client owns executive participation in reviews, timely remediation of approved items, maintaining baseline requirements (see Section 5C of the MSA), and all business decisions regarding risk acceptance.

Qualification Requirements

- Fundamentals baseline capabilities are included in Compliance; a separate Fundamentals subscription is not required
- Regulatory requirement, cyber insurance mandate, or executive-level risk governance need
- Executive participation required in quarterly vCISO reviews
- PTS security posture assessment completed
- Cyber liability insurance ($1M minimum recommended)

Transition Path

When the client hires internal IT staff, has documented roles, and maintains mature governance, PTS may recommend transitioning to Guardian Co-Managed. PTS security authority is maintained.

Guardian Co-Managed

"Enterprise-grade security for teams that already have IT."

Target Client

Organizations with qualified internal IT staff (IT Director or equivalent) that need enterprise-grade security tooling, escalation support, and strategic governance from PTS.

What's Included

- Security monitoring and SIEM services as specified in the SOW and Shared Responsibility Matrix
- Managed EDR across all endpoints
- Patch management coordination with internal IT (see Section 8 of the MSA)
- Tier 2/3 escalation support and engineering
- Firewall management (PTS-managed hardware per SOW)
- Monthly security posture review with internal IT
- Incident response coordination within scope (see Section 9B of the MSA)
- Quarterly strategic planning and governance review
- Optional: vCISO services if included in SOW

What's NOT Included

- Day-to-day helpdesk (client's internal IT handles this)
- Responsibility for client-controlled changes outside PTS-approved change management (see Section 8 of the MSA)
- Remediation of unauthorized changes by internal IT

Who Owns What

PTS owns security tooling, monitoring, governance, and escalation support. Client IT owns day-to-day operations, helpdesk, patch execution, and user support. Both parties share responsibility for incident response and strategic planning.

Qualification Requirements

- Qualified, dedicated internal IT personnel (IT Director or equivalent)

- Documented role separation between PTS and internal IT
- Established governance and change discipline (see Section 8 of the MSA)
- Acceptance of PTS security authority within defined scope
- Cyber liability insurance ($1M minimum recommended)

Transition Path

Guardian Co-Managed is a shared-responsibility service model, not a required next step after Compliance. If the client dissolves their internal IT team, a transition back to Guardian Fundamentals or Compliance may be appropriate.

SECTION 4: QUALIFICATION GATES

Tier transitions require meeting specific qualification criteria. PTS will advise when a transition is recommended.

Transition	Requirements
Ad-Hoc → Residential	Household must have consistent device footprint; agreement to PTS-approved security tools on all covered devices; signed SOW; residential terms governed by Section 4B of the MSA.
Residential → Fundamentals	Client starts or acquires a business; commercial systems enter the home/office environment; PTS assessment required to scope Fundamentals engagement.
Fundamentals → Compliance	Regulatory requirement identified (HIPAA, GLBA, CMMC, etc.); cyber insurance carrier mandates security governance; executive-level risk governance need; executive participation required in vCISO reviews; PTS security posture assessment completed.
Compliance → Co-Managed	Client hires qualified internal IT staff (IT Director or equivalent); documented roles and responsibilities between internal IT and PTS; governance maturity already established; PTS security authority maintained within defined scope.

SECTION 5: REGULATORY RIDER OPTIONS

Regulatory riders are available at the Guardian Compliance and Guardian Co-Managed tiers. These riders activate additional terms, protections, and service requirements for specific regulatory frameworks. The MSA contains the core rider terms; separately executed documents such as a HIPAA BAA may also be required.

Rider	MSA Section	Minimum Tier	Description
Healthcare / HIPAA	Section 10C of the MSA	Compliance	HIPAA/HITECH compliance services, BAA terms, PHI handling
Data Protection Addendum	Section 10B of the MSA	All tiers	Applies to Personal Data processing; not an optional Compliance-only upgrade
AI Services	Section 11C of the MSA	Compliance	Terms governing AI tool usage within managed environment
Custom Riders	As needed	Compliance	PTS develops custom regulatory riders as required — contact PTS

Section 10B applies across all Guardian tiers. HIPAA services require a separately executed BAA and the tier conditions in Section 10C. AI Services require express SOW scope under Section 11C; its tier rules and written exceptions apply. A general MSA reference does not replace a required BAA or other specific authorization.

SECTION 6: HOW PRICING WORKS

PTS pricing is determined per Statement of Work and is not published in this catalog. Each engagement is scoped individually based on the client's environment, risk profile, and selected tier. The pricing framework is governed by Section 12 of the MSA (Fees and Payment).

What Drives Pricing

- **Risk assumed** — Higher tiers mean PTS accepts more accountability and risk
- **Accountability accepted** — More PTS ownership of outcomes = higher investment
- **Service breadth** — Number of users, endpoints, locations, and complexity
- **Regulatory requirements** — Compliance and governance services add structure and cost

Optional Discounts

- Quarterly prepayment: 2% discount on monthly recurring fees
- Annual prepayment: 5% discount on monthly recurring fees

Price Adjustments

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.

SECTION 7: GETTING STARTED

Free Assessments

- Fundamentals, Compliance, and Co-Managed: Free initial IT and security assessment
- Residential: Free 30-minute home tech consultation

Onboarding Timelines

Onboarding procedures are governed by Section 7 of the MSA. Typical timelines are:

Tier	Typical Onboarding Timeline
Guardian Residential	1–2 weeks
Guardian Fundamentals	2–4 weeks
Guardian Compliance	4–6 weeks
Guardian Co-Managed	4–8 weeks

Contact Us

Phantom Technology Solutions, LLC

Rolling Prairie, Indiana

(800) 338-4474

support@phantomts.com

www.phantomts.com

DOCUMENT REFERENCE INDEX

You only need to sign **one document**: your Statement of Work (SOW). The MSA is incorporated by reference and available at https://www.phantomts.com/legal/msa.

Document	Status	Description
Master Services Agreement (MSA)	Reference only — not separately signed	Available at https://www.phantomts.com/legal/msa. Incorporated by reference into every SOW. Contains all terms covering tier definitions, security baseline, SLA, incident response, data protection, HIPAA, AI services, residential terms, and liability caps.
Statement of Work (SOW)	Required — both parties sign	Client-specific scope, covered assets, fees, term, and MSA incorporation acknowledgment. The SOW is the only document requiring Client signature.

Services Catalog	Reference only — no signature required	This document.
MSA Client Summary	Reference only — no signature required	Plain-language summary for clients.

This Services Catalog is provided for informational purposes. Service availability, scope, and pricing are subject to a signed Statement of Work (SOW). The MSA is incorporated by reference into every SOW and available at https://www.phantomts.com/legal/msa. This document does not constitute a binding offer or guarantee of service.