PHANTOM TECHNOLOGY SOLUTIONS, LLC

MASTER SERVICES AGREEMENT

Version 3.1 — Updated September 28, 2026

NOTICE OF INCORPORATION BY REFERENCE

This Master Services Agreement is incorporated by reference into every Statement of Work (SOW) executed with Phantom Technology Solutions, LLC. Clients are not required to separately sign this document. By executing a Statement of Work, Client acknowledges that Client has read, understood, and agreed to be bound by all terms contained in this Agreement. The current version of this Agreement is available at: https://www.phantomts.com/legal/msa

Rolling Prairie, Indiana

SECTION 1. PARTIES, EFFECTIVE DATE, AND PURPOSE

1.1 Parties.

This Master Services Agreement ("Agreement" or "MSA") is entered into by and between:

- Phantom Technology Solutions, LLC ("PTS," "Provider," "we," or "us"), an Indiana limited liability company organized and existing under the laws of the State of Indiana, with its principal place of business in Rolling Prairie, La Porte County, Indiana; and
- Client ("Client," "Customer," or "you"), the entity or individual identified in the applicable Statement of Work (SOW) executed with PTS. Client need not separately execute this Agreement; Client's signature on the applicable SOW constitutes full acceptance of, and agreement to be bound by, all terms of this Agreement. Where Client is a business entity, Client represents and warrants that the individual executing the applicable SOW has full authority to bind Client. Where Client is a natural person (e.g., a Guardian Residential client), Client represents and warrants that Client is at least eighteen (18) years of age and legally competent to enter into this Agreement.

1.2 Effective Date.

This Agreement is effective with respect to each Client as of the date on which Client executes the first Statement of Work referencing this Agreement (the "Effective Date"). Client's execution of a Statement of Work constitutes full acceptance of all terms herein. This Agreement does not require separate execution by Client.

1.3 Purpose.

This Agreement establishes the general terms and conditions under which PTS will provide information technology, cybersecurity, and related professional services to Client under the Phantom Guardian service model. PTS offers five distinct Guardian service tiers — Guardian Ad-Hoc, Guardian Residential, Guardian Fundamentals, Guardian Compliance, and Guardian Co-Managed — each designed for different client profiles, risk levels, and operational requirements. The specific tier, services, fees, and additional terms applicable to Client are defined in one or more Statements of Work ("SOWs") or Order Forms executed under this Agreement.

1.4 Binding Effect.

By executing any Statement of Work that references or incorporates this Agreement, Client acknowledges that Client has read this Agreement in its entirety (available at https://www.phantomts.com/legal/msa), understands its terms, and agrees to be bound by all provisions set forth herein. Client's signature on the applicable SOW is the sole execution required to form a binding, enforceable agreement incorporating all terms of this MSA. PTS has relied on this acknowledgment in agreeing to provide services.

1.5 Agreement Structure.

All terms and conditions governing this engagement are set forth directly in this Agreement. The following sections address specific subject areas:

- Section 3B — Guardian Tier Definitions and Service Alignment
- Section 4B — Residential Terms (Guardian Residential clients only)
- Section 5C — Security Baseline Requirements and Policies
- Section 6B — Service Level Targets and Support Terms
- Section 9B — Incident Response Scope and Fees
- Section 10B — Data Protection Addendum
- Section 10C — Healthcare and HIPAA Services (HIPAA clients only)
- Section 11C — AI Services (when included in SOW)
- Section 16.2 — Liability Cap Matrix

No separate exhibit documents are required. All applicable terms are contained herein.

SECTION 2. AGREEMENT STRUCTURE AND ORDER OF PRECEDENCE

2.1 Component Documents.

This Agreement, together with the applicable executed Statement of Work, constitutes the entire agreement between the parties. The component documents are:

1. Executed Statements of Work (SOWs) and Order Forms — signed by both parties;
2. This Master Services Agreement — incorporated by reference into each SOW; not separately signed.

2.2 Order of Precedence.

In the event of a conflict or inconsistency between an executed SOW and this Agreement, the SOW shall control to the extent of such conflict. All documents are to be read together and harmonized to the greatest extent possible.

2.3 Integration Clause.

This Agreement, together with all SOWs and Order Forms executed hereunder, constitutes the entire agreement between the parties and supersedes all prior and contemporaneous agreements, representations, understandings, negotiations, and discussions, whether oral or written. Without limiting the foregoing, the following are expressly excluded from this Agreement and shall have no contractual force or effect whatsoever:

- AI-generated proposals, estimates, scoping documents, or outputs of any kind;
- Chatbot outputs, automated responses, or auto-generated communications;
- Marketing materials, brochures, presentations, website content, case studies, or promotional communications;
- Informal communications, including emails, text messages, instant messages, social media communications, or verbal discussions, unless subsequently reduced to a written amendment executed in accordance with Section 18.3.

SECTION 3. DEFINITIONS AND INTERPRETATION

3.1 Definitions.

The following capitalized terms shall have the meanings set forth below when used in this Agreement. Capitalized terms used but not defined herein shall have the meanings ascribed to them in the applicable SOW, Exhibit, Schedule, or Addendum:

"Acceptance Period" means the fifteen (15) business day period following service commencement during which Client may review initial service delivery and notify PTS of material deficiencies, as described in Section 7.2.

"Agreement" means this Master Services Agreement, together with all SOWs and Order Forms executed hereunder, as may be amended from time to time in accordance with Section 18.3.

"Authorized Approver" means an individual designated by Client in the applicable SOW or in writing to PTS as having authority to approve changes, expenditures, scope modifications, or other actions on behalf of Client. Client may designate multiple Authorized Approvers and may modify designations by written notice to PTS.

"Authorized Representative" means an individual authorized to execute agreements, amendments, and other binding documents on behalf of a party.

"Baseline Requirements" means the minimum technical, operational, and security standards applicable to Client's environment as set forth in Section 5C of this Agreement (Security Baseline Requirements and Policies), as may be updated by PTS from time to time in accordance with Section 5C.4 of this Agreement.

"Business Hours" means the standard support hours applicable to Client's Guardian Tier as specified in the applicable SOW and Section 6B of this Agreement. Unless otherwise specified, Business Hours are Monday through Friday, 9:00 AM to 5:00 PM Eastern Time, excluding PTS-observed holidays.

"Client Data" means all data, files, content, communications, databases, records, and information owned or controlled by Client that is stored on, processed by, or transmitted through systems managed or accessed by PTS in the course of providing Covered Services.

"Client IP" means all intellectual property owned by Client prior to or independent of this Agreement, including Client Data, Client-created content, Client's trade secrets, trademarks, and proprietary business processes.

"Client Responsibilities" means the obligations, actions, cooperation, and commitments required of Client as set forth in Sections 5 and 5B of this Agreement, the applicable SOW, Section 3B of this Agreement, and Section 5C of this Agreement.

"Compliance Owner" means the individual designated by a Guardian Compliance client as the internal business owner responsible for compliance-related decisions, as required by Section 3B.6.7 of this Agreement.

"Confidential Information" means all non-public information disclosed by one party to the other in connection with this Agreement, whether oral, written, electronic, visual, or in any other form, that is designated as confidential or that a reasonable person would understand to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes, without limitation, business plans, financial data, customer lists, vendor lists, technical data, trade secrets, pricing, proposals, security configurations, network architecture, authentication credentials, vulnerability assessments, incident reports, and the terms and pricing of any SOW or Order Form. The text of this Agreement, as published by PTS, is not Confidential Information.

"Covered Assets" means the specific hardware, software, systems, devices, users, network components, and cloud services identified in the applicable SOW as being within the scope of Covered Services. Only assets expressly identified are Covered Assets; all other assets are excluded.

"Covered Services" means the specific services to be provided by PTS to Client under the applicable SOW, as determined by Client's Guardian Tier and any additional services specified therein.

"Cure Period" means the thirty (30) day period following delivery of a written notice of material breach during which the breaching party may cure the breach, as described in Section 13.6.

"Dispute Notice" means the written notice delivered by the aggrieved party describing a dispute, the specific provisions at issue, and the relief sought, as described in Section 19.2.

"Early Termination Fee" means the fee payable upon early termination for convenience as calculated in Section 13.7 of this Agreement (or Section 4B.9 for Residential clients).

"Effective Date" means the date on which this Agreement becomes effective, as specified in Section 1.2.

"Emergency Change" means a change to the Client environment that must be implemented immediately to restore service, prevent imminent security compromise, or address a critical system failure, as further described in Section 8 of this Agreement.

"Force Majeure Event" has the meaning set forth in Section 18.1.

"Guardian Ad-Hoc" means the PTS service tier providing reactive, time-and-materials-based IT support without ongoing management, monitoring, or SLA commitments, as described in Section 3B.3 of this Agreement.

"Guardian Co-Managed" means the PTS service tier designed for organizations with qualified internal IT staff, providing shared-responsibility security, escalation, and governance services, as described in Section 3B.7 of this Agreement.

"Guardian Compliance" means the PTS service tier providing all Guardian Fundamentals services plus vCISO-led security governance, compliance framework alignment, risk assessment, and regulatory readiness services, as described in Section 3B.6 of this Agreement.

"Guardian Fundamentals" means the PTS service tier providing fully managed IT services for organizations without internal IT staff, including endpoint management, Microsoft 365 administration, security operations, and user support, as described in Section 3B.5 of this Agreement.

"Guardian Residential" means the PTS service tier providing managed personal and household IT and cybersecurity services for individuals and households, as described in Section 3B.4 and Section 4B of this Agreement.

"Guardian Tier" means one of the five PTS service tiers: Guardian Ad-Hoc, Guardian Residential, Guardian Fundamentals, Guardian Compliance, or Guardian Co-Managed, each as defined in Section 3B of this Agreement.

"Incident" means an unplanned interruption to, or reduction in the quality of, a Covered Service, or an event that could reasonably be expected to cause such interruption or reduction.

"Initial Term" means the initial term of this Agreement or an applicable SOW, as specified in Section 13.1 or the applicable SOW. The default Initial Term is twelve (12) months unless otherwise specified.

"Order Form" means a document executed by the parties that references this Agreement and specifies services, fees, quantities, or other commercial terms, but does not contain the full detail of a Statement of Work.

"Out-of-Scope Services" means any services, tasks, responsibilities, or activities not expressly included as Covered Services in the applicable SOW, including but not limited to the items listed in Section 4.3 of this Agreement.

"Personal Data" means any information relating to an identified or identifiable natural person, as defined under applicable data protection laws, including the Indiana Consumer Data Protection Act (Ind. Code § 24-15), the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.), and the General Data Protection Regulation (EU Regulation 2016/679).

"Provider IP" means all intellectual property owned by or licensed to PTS, including tools, scripts, software, methodologies, processes, templates, frameworks, documentation, training materials, and know-how

developed by PTS prior to or independent of this Agreement, or developed by PTS in the course of providing services that are of general applicability and do not incorporate Client IP or Client Data.

"PTS Standard Stack" means the curated set of approved third-party tools, platforms, and technologies that PTS has selected, vetted, and standardized for use across its client base, as described in Section 11B of this Agreement.

"Renewal Term" means each successive renewal period following the Initial Term, as described in Section 13.2 of this Agreement.

"Restoration Fee" means the fee that PTS may charge to cover the costs of re-onboarding, re-assessment, re-configuration, or security verification following a service suspension, as described in Section 13.5.

"Security Event" means any event that compromises, or reasonably appears to compromise, the confidentiality, integrity, or availability of Client Data, Covered Assets, or Covered Services, including without limitation unauthorized access, malware infections, ransomware deployment, data exfiltration, denial-of-service attacks, phishing compromises, and credential theft.

"Service Acceptance" means Client's acknowledgment that services have been properly delivered in material conformity with the SOW, either by express written confirmation or by deemed acceptance as set forth in Section 7.2 of this Agreement.

"Shared Responsibility Matrix" means the document agreed between PTS and a Guardian Co-Managed client that defines the allocation of IT and security responsibilities between PTS and the client's internal IT team.

"SOW" or "Statement of Work" means a document executed by both parties that references this Agreement and describes the specific Covered Services, Covered Assets, Guardian Tier, fees, term, and other terms applicable to a specific service engagement with Client.

"Standard Change" means a pre-approved, low-risk, routine change to the Client environment performed in accordance with established procedures as described in Section 8.1 of this Agreement.

"Transition Period" means the period of up to thirty (30) days following the effective date of termination during which PTS provides transition assistance as described in Section 7.3 of this Agreement.

"72-Hour Notification Target" means the service objective for Guardian Compliance clients under which PTS uses commercially reasonable efforts to notify Client within seventy-two (72) hours of confirming a Security Event, as described in Section 9.2.

3.2 Interpretation.

In this Agreement:

- "including" means "including without limitation" unless otherwise expressly specified;
- references to "Sections," "Exhibits," and "Schedules" are to sections of, and exhibits and schedules to, this Agreement unless otherwise specified;
- headings and captions are for convenience of reference only and shall not affect the interpretation or construction of this Agreement;
- words in the singular include the plural and vice versa; references to any gender include all genders;
- references to "days" mean calendar days unless "business days" is expressly specified;
- this Agreement shall not be construed against or in favor of any party by reason of the authorship or drafting of any provision hereof;
- references to any law, regulation, statute, or ordinance include any amendments, successors, re-enactments, or replacements thereto;
- references to monetary amounts are to United States Dollars unless otherwise specified.

3.3 Construction of Lists.

Where this Agreement includes a list of items following the word "including" or similar terms, such list is illustrative and not exhaustive unless the context expressly indicates otherwise.

3.4 Time Periods.

Where this Agreement specifies a period of days: (a) for periods stated in "calendar days" or simply "days," the period begins on the day after the triggering event and includes all calendar days, including weekends and holidays; (b) for periods stated in "business days," the period begins on the next business day after the triggering event, and weekends and PTS-observed holidays are excluded; (c) if the last day of any period falls on a weekend or PTS-observed holiday, the period extends to the next business day.

3.5 Good Faith.

The parties shall act in good faith in the performance of their respective obligations under this Agreement. Neither party shall unreasonably withhold, delay, or condition any approval, consent, or cooperation required under this Agreement unless a different standard is expressly stated (e.g., "sole discretion").

SECTION 3B. GUARDIAN TIER DEFINITIONS AND SERVICE ALIGNMENT

3B.1 Guardian Tier Framework

Phantom Technology Solutions, LLC ("PTS") delivers information technology and cybersecurity services through the Phantom Guardian service model. The Guardian model comprises five distinct service tiers, each designed to address the unique needs, risk profiles, and operational requirements of different client categories. The five Guardian Tiers, ordered from least to most comprehensive, are:

Tier	Target Client	Service Model	PTS Role	Liability Cap
Guardian Ad-Hoc	Organizations/individuals not ready for managed IT	Reactive, time & materials	On-demand technician	Lesser of service fees or $5,000
Guardian Residential	Households, remote workers, executive homes	Consumer managed services	Personal IT advisor	Lesser of 2 months fees or $10,000
Guardian Fundamentals	SMBs (1–50 users), no internal IT	Fully managed IT	Client's IT department	Lesser of 3 months fees or $25,000
Guardian Compliance	Regulated or insured organizations	Managed IT + security governance	vCISO / security authority	Lesser of 6 months fees or $75,000
Guardian Co-Managed	Organizations with internal IT staff	Shared responsibility	Security partner / escalation	Lesser of 6 months fees or $75,000

Each tier has specific eligibility requirements, included and excluded services, client responsibilities, and liability alignment as detailed in the sections below. The applicable tier is specified in the Client's Statement of Work (SOW). Clients may operate under only one tier at a time per SOW unless otherwise agreed in writing. Clients may have multiple SOWs at different tiers (for example, a Residential SOW for the owner's home and a Fundamentals SOW for the business).

The Guardian Tier Framework is designed to be scalable. Clients are encouraged to start at the tier that matches their current needs and evolve to higher tiers as their requirements, regulatory obligations, or organizational maturity change.

3B.2 General Tier Conditions (All Tiers)

3B.2.1 Scope Limitation

Services under each Guardian Tier are limited to the Covered Services and Covered Assets identified in the applicable SOW. PTS is not responsible for systems, devices, users, networks, cloud services, or environments not expressly included in the SOW. Any services not expressly included are Out-of-Scope Services as defined in Section 4.3 of this Agreement.

3B.2.2 Professional Standards

PTS shall perform all services with commercially reasonable care consistent with applicable industry standards and best practices for managed IT and cybersecurity service providers. PTS does not guarantee any specific outcome, including prevention of security breaches, system uptime, data recovery, or regulatory compliance. PTS's obligation is one of reasonable effort and professional diligence, not one of absolute result.

3B.2.3 Client Cooperation

Effective service delivery requires Client's active cooperation. Client shall provide timely access, accurate and complete information, prompt decisions, and all approvals necessary for PTS to perform its obligations. Service

delivery timelines, quality, and outcomes depend directly on Client's adherence to its responsibilities. Delays or deficiencies attributable to Client shall not constitute a breach by PTS.

3B.2.4 Baseline Compliance

Each Guardian Tier has specific Baseline Requirements as set forth in Section 5C of this Agreement (Security Baseline Requirements and Policies). Client must achieve and maintain compliance with the applicable Baseline Requirements throughout the term of the engagement. Non-compliance may result in reduced service quality, adjusted liability caps, suspension of services, or termination as described in this Agreement.

3B.2.5 Fees and Payment

Fees for each tier are defined in the applicable SOW or Order Form and are governed by Section 12 of this Agreement. Fees may include monthly recurring charges, onboarding fees, project fees, and time-and-materials charges for out-of-scope work. Annual price adjustments are governed by Section 12.11 of this Agreement.

3B.2.6 Tools and Agents

PTS may deploy monitoring agents, endpoint detection and response (EDR) tools, remote management and monitoring (RMM) software, security tools, and other agents on Covered Assets as necessary to deliver services. Client must permit installation and continuous operation of these tools and must not interfere with, disable, uninstall, or circumvent them. Interference with PTS tools may void PTS's service delivery obligations and liability.

3B.2.7 No Legal, Accounting, or Insurance Services

PTS is not a law firm, accounting firm, insurance company, insurance broker, or licensed auditor. PTS's services, including vCISO advisory services at the Compliance tier, do not constitute legal advice, accounting services, insurance advice, insurance products, or formal audit opinions. Clients requiring such services should engage appropriately licensed professionals. PTS may provide introductions or referrals to such professionals as a courtesy, but PTS does not warrant or guarantee such professionals' services.

3B.2.8 Service Modifications

PTS reserves the right to modify service delivery methods, tools, platforms, and procedures from time to time, provided that such modifications do not materially reduce the scope or quality of Covered Services. PTS shall provide reasonable notice of material service delivery changes.

3B.3 Guardian Ad-Hoc

3B.3.1 Description

Guardian Ad-Hoc provides reactive, on-demand IT support on a time-and-materials (T&M) basis. Ad-Hoc is expressly not a managed service. There is no ongoing management, monitoring, proactive maintenance, security operations, or SLA commitment of any kind. Client retains one hundred percent (100%) responsibility for all aspects of the IT environment, including security, backup, updates, licensing, and compliance. PTS acts solely as an on-demand technician responding to specific requests.

3B.3.2 Target Client

Organizations or individuals that: (a) are not ready or willing to commit to an ongoing managed IT engagement; (b) have minimal IT needs that do not justify a managed service; (c) need occasional technical assistance for specific issues, projects, or assessments; or (d) are evaluating PTS services before committing to a managed tier.

3B.3.3 Included Services

- Reactive break-fix support for specific issues on a per-incident, per-request basis;
- Technical consultation and advisory services by appointment;
- Project-based IT work as defined in individual SOWs or Order Forms (e.g., network setup, server installation, migration assistance);

- Basic technology assessments and environment reviews;
- Ad-hoc procurement assistance (recommendations only; Client purchases directly).

3B.3.3.1 2026 Labor Rate Card

All Ad-Hoc services are billed at the following time-and-materials rates, confirmed per engagement in the applicable SOW or Order Form:

Service Type	Rate
Residential In-Shop	$135 / hour
Residential On-Site	$135 / hour
Remote (standard)	$180 / hour
On-Site (standard)	$180 / hour
Emergency (during business hours / scheduled after-hours)	$225 / hour
Emergency (after hours / holidays)	$270 / hour

Rates are billed in one-hour minimum increments, then in thirty (30) minute increments thereafter. Travel time for Ad-Hoc on-site services is billed at the applicable on-site rate. Travel time is not billed for on-site support included in a managed Guardian Tier within the service area defined in the applicable SOW. Final per-engagement rates are confirmed in the SOW or Order Form.

3B.3.4 Excluded Services

- Ongoing monitoring, alerting, proactive management, or health checks;
- Endpoint detection and response (EDR) or any managed security service;
- Backup management, disaster recovery planning, or business continuity;
- Patch management, update management, or vulnerability management;
- SLA-based support with defined response or resolution time commitments;
- Security governance, compliance services, vCISO, or risk assessment;
- Incident response planning or coordination;
- Microsoft 365 or cloud platform administration;
- User onboarding/offboarding processes;
- Technology business reviews or strategic planning.

3B.3.5 Client Responsibilities

- Maintain and manage all aspects of the IT environment independently;
- Contact PTS to initiate each service request; PTS does not monitor or proactively engage;
- Provide an accurate description of issues and full cooperation during resolution;
- Authorize all work and associated fees before PTS commences work;
- Ensure all software is properly licensed and hardware is in serviceable condition;
- Maintain data backups independently; PTS is not responsible for data loss.

3B.3.6 Eligibility

No minimum eligibility requirements beyond execution of the MSA and an applicable SOW or Order Form for each engagement. Ad-Hoc clients are not subject to Baseline Requirements (Section 5C of this Agreement) beyond the Universal Baseline.

3B.3.7 Liability Alignment

PTS's liability for Guardian Ad-Hoc services is limited to the lesser of: (a) total fees paid by Client for the specific engagement giving rise to the claim, or (b) $5,000. No SLA credits apply. Ad-Hoc services are provided on a best-efforts basis without any warranty of outcome.

3B.4 Guardian Residential

3B.4.1 Description

Guardian Residential provides managed personal and household IT and cybersecurity services for individuals, families, households, remote workers, and executive home environments. Residential services are consumer services — they are expressly not commercial managed IT services. All Residential services are for personal and household use only.

3B.4.2 Target Client

Individuals, families, and households seeking: (a) managed security and IT support for personal devices and home networks; (b) protection for remote work environments where the employer does not provide personal device security; (c) executive home office environments requiring elevated consumer security; or (d) individuals with significant personal digital assets or household members with elevated privacy needs.

3B.4.3 Included Services

Included services are as specified in the applicable SOW and may include:

- Endpoint security management (EDR/antivirus) for covered household devices;
- Home network security monitoring and management for covered network equipment;
- Patch and update management for covered devices;
- Password management and secure credential storage (household members);
- Dark web monitoring for household email addresses and identity information;
- Remote helpdesk support during Business Hours;
- Annual security assessment of covered devices and home network;
- Security awareness guidance tailored to household needs;
- Basic incident response for covered devices (malware removal, access restoration).

3B.4.4 Excluded Services

- Commercial or business-use devices or networks;
- Devices not listed as Covered Assets in the applicable SOW;
- Business compliance services, vCISO, or regulatory compliance advisory;
- Legal or insurance services;
- Physical on-site services beyond a reasonable geographic radius agreed in the SOW;
- Data forensics, litigation support, or digital evidence preservation;
- Services for employer-issued or business-controlled devices.

3B.4.5 Client Responsibilities

- Maintain supported operating systems and device firmware;
- Permit installation and operation of PTS security agents on covered devices;
- Ensure all household members aged 18+ acknowledge PTS monitoring as described in Section 4B.4;
- Notify PTS promptly if a covered device is lost, stolen, or compromised;
- Use covered services for personal and household purposes only;
- Maintain internet service at the household at Client's cost.

3B.4.6 Eligibility

Enrollment in Guardian Residential requires: (a) all covered devices must meet minimum OS and hardware requirements set forth in Section 5C and Section 4B.3 of this Agreement; (b) Client must be an individual (natural person), not a business entity; (c) covered services must be for personal and household use only. If a covered household includes devices used primarily for business purposes, those devices require enrollment under a commercial tier.

3B.4.7 Liability Alignment

PTS's liability for Guardian Residential services is limited to the lesser of: (a) two (2) months of recurring fees at the then-current rate, or (b) $10,000, per the Liability Cap Matrix in Section 16.2 of this Agreement. Additional residential-specific liability terms are set forth in Section 4B.10 of this Agreement.

3B.5 Guardian Fundamentals

3B.5.1 Description

Guardian Fundamentals provides fully managed IT services for small and medium-sized businesses (SMBs) without qualified internal IT staff. Under Fundamentals, PTS serves as the client's complete IT department, providing endpoint management, network monitoring, Microsoft 365 administration, patch management, managed security operations, backup and recovery, and user support.

3B.5.2 Target Client

Small and medium-sized businesses and organizations that: (a) have between 1 and 50 users; (b) do not have qualified internal IT staff and rely on PTS as their IT department; (c) are not subject to complex regulatory requirements (if subject to such requirements, Guardian Compliance may be more appropriate); (d) need comprehensive IT management without the cost of internal IT personnel.

3B.5.3 Included Services

Included services are as specified in the applicable SOW and typically include:

- Endpoint Management: monitoring, patching, and lifecycle management for all Covered Assets;
- Microsoft 365 Administration: tenant management, user licensing, Exchange, Teams, SharePoint, and OneDrive administration, and Microsoft 365 security configuration;
- Managed EDR: enterprise-grade endpoint detection and response for all Covered Assets;
- Managed MDR/SOC: 24/7 managed detection and response with a security operations center;
- Email Security: spam filtering, anti-phishing, and email threat protection;
- DNS/Web Filtering: DNS-layer content filtering and threat blocking;
- Cloud Backup and Recovery: image-based backup for endpoints and servers; recovery testing;
- Network Monitoring: monitoring of core network infrastructure (routers, switches, firewalls);
- Helpdesk Support: remote and on-site user support during Business Hours within the support allowance defined in the applicable SOW, with no travel charges within the service area defined in the SOW; ticketing system access;
- Security Awareness Training: annual phishing simulation and security training platform;
- Dark Web Monitoring: credential monitoring for business domains;
- Password Management: enterprise password manager licenses;
- User Onboarding/Offboarding: standard onboarding and offboarding workflows;
- Technology Business Reviews: quarterly TBRs with assigned PTS account manager.

3B.5.4 Excluded Services

- vCISO advisory, compliance framework alignment, or formal risk assessments (available at Guardian Compliance tier);
- On-site services outside the service area defined in the SOW, or beyond the support allowance defined in the SOW (billed separately at the rates in the SOW);
- Server hardware procurement, installation, or physical racking;
- Custom software development or application management;
- Telecommunications or VoIP services (unless specified in SOW);
- Services for systems, devices, or users not identified as Covered Assets in the SOW.

3B.5.5 Client Responsibilities

- Maintain all Covered Assets in compliance with Baseline Requirements (Section 5C);
- Provide PTS with timely access, approvals, and information to deliver services;
- Notify PTS promptly of new users, devices, or changes to the IT environment;
- Follow PTS-established security procedures and acceptable use policies;
- Do not permit installation of unauthorized software or tools on Covered Assets without PTS approval;
- Designate an Authorized Approver for changes and expenditures;
- Maintain business continuity plans for operations during IT outages.

3B.5.6 Eligibility

Enrollment in Guardian Fundamentals requires: (a) all Covered Assets must meet the Baseline Requirements in Section 5C; (b) Client must accept the PTS Standard Stack (Section 11B); (c) Client must not have internal IT staff with administrative access to covered systems unless explicitly agreed in writing. Clients with qualified internal IT staff should evaluate Guardian Co-Managed.

3B.5.7 Liability Alignment

PTS's liability for Guardian Fundamentals services is limited to the lesser of: (a) three (3) months of recurring fees at the then-current rate, or (b) $25,000, per the Liability Cap Matrix in Section 16.2 of this Agreement.

3B.6 Guardian Compliance

3B.6.1 Description

Guardian Compliance provides all Guardian Fundamentals services plus vCISO-led security governance, compliance framework alignment, risk assessment and management, security awareness programs, tabletop exercises, incident response coordination, and regulatory readiness support. Guardian Compliance is designed for regulated, insured, or compliance-sensitive organizations that require a formal security program in addition to managed IT.

3B.6.2 Target Client

Organizations that: (a) are subject to regulatory frameworks (HIPAA, GLBA, FINRA, CMMC, SOC 2, CIS Controls, NIST CSF, or similar); (b) carry or are seeking cyber liability insurance requiring demonstrated security controls; (c) have experienced a security incident and are implementing remediation; (d) have clients, partners, or vendors requiring demonstrated security compliance; or (e) have organizational risk exposure that warrants a formal security governance program.

3B.6.3 Included Services

In addition to all Guardian Fundamentals services, Guardian Compliance typically includes:

- Virtual Chief Information Security Officer (vCISO): named vCISO providing strategic security leadership, risk prioritization, and board/executive reporting;

- Annual Security Risk Assessment: formal risk assessment aligned to applicable frameworks;
- Compliance Framework Alignment: mapping of security controls to CIS Controls, NIST CSF, HIPAA Security Rule, or other applicable frameworks as specified in the SOW;
- Security Policy Development: development and maintenance of information security policies, procedures, and standards;
- Tabletop Exercises: annual tabletop exercise simulating a cybersecurity incident scenario;
- Phishing Simulation Program: monthly or quarterly simulations with reporting and remediation;
- Incident Response Planning: formal IR plan development and maintenance;
- Cyber Insurance Readiness Support: assistance with cyber insurance applications and renewals;
- 72-Hour Security Event Notification Target: as described in Section 9.2 of this Agreement;
- Regulatory Readiness Reporting: periodic reporting aligned to applicable regulatory requirements.

3B.6.4 Excluded Services

- Legal advice, formal legal opinions, or legal representation;
- Formal audit services, certified audit reports, or attestations (ISO 27001, SOC 2 Type II formal certification);
- Insurance brokerage, insurance products, or claims handling;
- Physical security, surveillance, or access control hardware;
- Services for systems, users, or networks not identified as Covered Assets in the SOW.

3B.6.5 Client Responsibilities

In addition to all Guardian Fundamentals client responsibilities, Guardian Compliance clients must:

- Designate a Compliance Owner as internal business sponsor for the compliance program;
- Engage in quarterly or more frequent reviews with the vCISO;
- Implement and maintain policies and procedures recommended by PTS within agreed timelines;
- Participate in tabletop exercises, risk assessments, and compliance reviews;
- Provide accurate and complete information about regulatory requirements, audit schedules, and compliance deadlines;
- Notify PTS promptly of any regulatory audit, inquiry, or investigation;
- Implement remediation items within timelines agreed in the risk register or remediation plan.

3B.6.6 Eligibility

Enrollment in Guardian Compliance requires: (a) all Covered Assets must meet the Baseline Requirements in Section 5C; (b) Client must accept the PTS Standard Stack (Section 11B); (c) Client must designate a Compliance Owner prior to commencement of compliance services; (d) for HIPAA-covered entities, Client must execute the BAA and activate Section 10C of this Agreement prior to commencement of HIPAA-related services.

3B.6.7 Compliance Owner Requirement

Each Guardian Compliance client must designate an individual as Compliance Owner. The Compliance Owner is the internal business owner responsible for: (a) making compliance-related decisions; (b) approving risk acceptance decisions; (c) ensuring internal implementation of recommended controls; (d) serving as the primary point of contact for PTS's vCISO. If the Compliance Owner is unavailable, Client must designate an alternate. PTS's vCISO services are contingent on the Compliance Owner's active participation.

3B.6.8 Liability Alignment

PTS's liability for Guardian Compliance services is limited to the lesser of: (a) six (6) months of recurring fees at the then-current rate, or (b) $75,000, per the Liability Cap Matrix in Section 16.2 of this Agreement. The

enhanced liability cap reflects the elevated scope of services and PTS's deeper integration into the client's security governance.

3B.7 Guardian Co-Managed

3B.7.1 Description

Guardian Co-Managed is a shared-responsibility IT and cybersecurity service designed for organizations with qualified internal IT staff. Under Co-Managed, PTS and the client's internal IT team divide responsibilities based on a negotiated Shared Responsibility Matrix. PTS provides enterprise-grade security tooling, managed security operations, strategic security governance, escalation support, and lifecycle management, while the client's internal team retains primary responsibility for day-to-day IT operations.

3B.7.2 Target Client

Organizations that: (a) have qualified internal IT personnel managing day-to-day IT operations; (b) need enterprise-grade security tooling and a 24/7 managed security operations center without a fully outsourced IT model; (c) require security governance, compliance alignment, and strategic security leadership; (d) need specialized skills (security engineering, incident response, vCISO) to supplement their internal team.

3B.7.3 Shared Responsibility Matrix

PTS and Client shall execute a Shared Responsibility Matrix (SRM) as part of the onboarding process. The SRM defines which responsibilities are owned by PTS, which are owned by Client's internal IT, and which are shared. The SRM is incorporated into and made part of the applicable SOW. Changes to the SRM require mutual written agreement. If Client's internal IT circumstances change (e.g., staff turnover, reorganization), Client shall promptly notify PTS and the parties shall revise the SRM accordingly.

3B.7.4 Included Services

Included services are determined by the Shared Responsibility Matrix and the applicable SOW, and typically include:

- Managed EDR/MDR/SOC: 24/7 managed endpoint detection, response, and security operations center;
- Security Tooling and Stack Management: deployment, management, and maintenance of PTS Standard Stack security tools;
- vCISO Services: strategic security leadership, risk prioritization, and governance (as specified in SOW);
- Compliance Support: framework alignment, risk assessment, and compliance roadmap (as specified in SOW);
- Escalation and L3/L4 Support: advanced technical escalation for complex issues beyond internal team capacity;
- Vulnerability and Patch Management: vulnerability scanning, patch prioritization, and lifecycle management;
- Incident Response Coordination: PTS leads or supports incident response per the SRM and Section 9B;
- Technology Business Reviews: quarterly or more frequent TBRs with the PTS vCISO or account manager.

3B.7.5 Client Responsibilities

In addition to general tier responsibilities, Guardian Co-Managed clients must:

- Maintain a qualified internal IT team as described in the SRM;
- Follow PTS-prescribed security configurations, procedures, and policies on all Covered Assets;
- Notify PTS of personnel changes affecting IT roles (new hires, departures, role changes) within five (5) business days;
- Participate in quarterly TBRs and annual risk assessments;

- Implement remediation items within timelines agreed in the SRM or risk register;
- Not make material changes to Covered Assets without PTS notification and coordination;
- Ensure internal IT staff complete PTS-provided security onboarding and comply with PTS security procedures.

3B.7.6 Eligibility

Enrollment in Guardian Co-Managed requires: (a) Client must have at least one (1) qualified internal IT staff member; (b) all Covered Assets must meet Baseline Requirements in Section 5C; (c) Client must accept the PTS Standard Stack for security tooling (Section 11B); (d) the parties must execute a Shared Responsibility Matrix prior to service commencement.

3B.7.7 Liability Alignment

PTS's liability for Guardian Co-Managed services is limited to the lesser of: (a) six (6) months of recurring fees at the then-current rate, or (b) $75,000, per the Liability Cap Matrix in Section 16.2 of this Agreement. PTS's liability is reduced proportionally for incidents attributable to actions or omissions of Client's internal IT staff, as further described in Section 16.2 of this Agreement.

SECTION 4. SCOPE AND SERVICE MODEL

4.1 Guardian Tier Framework.

PTS provides information technology and cybersecurity services under the Phantom Guardian model through five distinct service tiers, each designed to address the unique needs, risk profiles, and operational requirements of different client categories. The five Guardian Tiers, ordered from least to most comprehensive, are:

- Guardian Ad-Hoc: Reactive, time-and-materials IT support. No ongoing management, monitoring, proactive maintenance, or SLA commitments. Client retains one hundred percent (100%) responsibility for all aspects of the IT environment. Expressly not a managed service.
- Guardian Residential: Managed personal and household IT and cybersecurity services for individuals and households. Consumer service — not a commercial managed service. Services are for personal and household use only.
- Guardian Fundamentals: Fully managed IT services for organizations without internal IT staff. PTS serves as the client's IT department, providing endpoint management, Microsoft 365 administration, patch management, managed EDR, backup and recovery, network monitoring, and user support.
- Guardian Compliance: All Guardian Fundamentals services plus vCISO-led security governance, compliance framework alignment (CIS Controls / NIST CSF), annual risk assessment, security awareness training, phishing simulations, incident response coordination, compliance roadmap, tabletop exercises, and cyber insurance readiness support.
- Guardian Co-Managed: Shared-responsibility IT and security services for organizations with qualified internal IT staff. PTS provides enterprise-grade security tooling, governance, escalation support, and lifecycle management.

The complete definitions, included services, excluded services, client responsibilities, eligibility requirements, and liability alignment for each tier are set forth in Section 3B of this Agreement (Guardian Tier Definitions and Service Alignment).

4.2 Covered Services.

The specific services to be provided by PTS are defined expressly in the applicable SOW and are limited to those services. PTS shall not be obligated to perform any services not expressly included in an executed SOW, regardless of any discussions, proposals, expectations, prior course of dealing, or industry custom.

4.3 Out-of-Scope Services.

Unless expressly included in an executed SOW, the following are Out-of-Scope Services and are not included in any Guardian Tier (this list is illustrative, not exhaustive):

- Procurement, purchase, leasing, or licensing of hardware, software, or third-party services on behalf of Client (unless expressly specified in the SOW);
- Cabling, wiring, rack-and-stack, or hardware installation, and on-site services not included in Client's Guardian Tier or SOW;
- Development, customization, coding, or programming of custom software applications;
- Legacy system support for end-of-life hardware or software not meeting Baseline Requirements;
- Legal advice, accounting services, insurance brokerage, audit services, or regulatory certification;
- Data recovery from failed media or devices not covered by PTS-managed backup;
- Remediation of issues caused by unauthorized changes, non-approved third parties, or Client's internal staff acting outside agreed procedures;
- Services for systems, devices, users, or networks not identified as Covered Assets in the SOW;
- Forensic investigation, digital evidence preservation, litigation support, or expert witness services;

- Physical security, surveillance systems, access control hardware, environmental controls, or facilities management;
- Training of Client staff beyond security awareness training included in the Guardian Compliance tier;
- Website development, hosting, content management, or search engine optimization;
- Telecommunications services, VoIP provisioning, or carrier management (unless specified in SOW).

4.4 No Guaranteed Outcomes.

Client acknowledges and agrees that PTS does not and cannot guarantee any specific outcomes, including but not limited to: (a) prevention of all security breaches, cyberattacks, data loss, or unauthorized access; (b) elimination of all vulnerabilities or security risks; (c) uninterrupted system availability, uptime, or performance; (d) regulatory compliance, audit outcomes, certification, or accreditation; (e) recovery of lost, corrupted, or encrypted data; or (f) specific business results or return on investment. PTS's obligations are limited to performing Covered Services with commercially reasonable care consistent with applicable industry standards and best practices.

4.5 Residential Tier Limitation.

Guardian Residential services are intended exclusively for personal and household use. Covered devices and services under the Residential tier shall not be used for business operations, commercial purposes, or the storage or processing of regulated data (including data subject to HIPAA, GLBA, PCI DSS, FERPA, or similar regulatory frameworks). If Client's household includes devices used for commercial activities, Client must notify PTS promptly and may be required to upgrade to the appropriate commercial Guardian Tier. Continued use of Residential services for commercial purposes after PTS notification constitutes a material breach of this Agreement. The specific terms governing Residential services are set forth in Section 4B of this Agreement.

SECTION 4B. RESIDENTIAL TERMS

APPLICABILITY: This Section 4B applies exclusively to clients enrolled in the Guardian Residential tier. Clients enrolled in any other Guardian Tier are not subject to this Section.

This Section 4B sets forth PTS's specific terms governing the provision of household and personal IT services under the Guardian Residential tier. These consumer service terms supplement the MSA with provisions tailored to the consumer nature of Residential services.

4B.1 Purpose and Scope

This Residential Terms section governs the provision of household and personal IT services under the Guardian Residential tier. Guardian Residential services are consumer services intended for personal and household use. They are not commercial managed IT services. This section supplements the MSA with terms tailored to the consumer nature of Residential services. Client's use of Residential services is also subject to the acceptable use requirements of Section 5B of the MSA.

4B.2 Household Coverage

Guardian Residential services cover the specific household devices and users identified in the applicable SOW. Coverage includes only those devices and household members expressly listed. To add devices or household members to the coverage, Client must request an amendment to the SOW. PTS will confirm eligibility of new devices (supported OS, device type) before adding them to coverage. PTS is not responsible for devices or household members not identified in the SOW.

4B.3 Device Eligibility

Covered devices must meet the Guardian Residential Baseline Requirements set forth in Section 5C of the MSA. The following table summarizes device eligibility requirements:

Category	Requirement	Exclusion
Operating System	Windows 11; a macOS version currently supported by Apple with security updates; current Ubuntu LTS	End-of-life OS versions (Windows 10 and earlier, unsupported macOS versions) are not eligible
Endpoint Agent Compatibility	Device must be capable of running PTS-approved endpoint security and monitoring agents without material degradation	Devices that cannot run required agents will be excluded; Client may remediate and request re-evaluation
Mobile Devices	Standard iOS and Android devices meeting agent requirements	Jailbroken or rooted devices are not eligible for coverage
Performance	Sufficient storage and processing capacity to operate PTS security tools without material impact on device performance	Devices with critically degraded hardware may be excluded at PTS's reasonable discretion
Device Ownership	Devices must be owned by or regularly used by Client and household members identified in the SOW	Commercial, employer-issued, or business-use devices may not qualify for Residential coverage

PTS reserves the right to exclude devices that do not meet eligibility requirements. Client may remedy ineligible devices and request re-evaluation. PTS will confirm device eligibility within ten (10) business days of a re-evaluation request.

4B.4 Household Member Authorization

All household members aged eighteen (18) or older who will use covered devices or services must acknowledge that they are subject to PTS's monitoring policies as described in Section 11 of the MSA. Client is responsible for informing household members of the monitoring and obtaining their acknowledgment. PTS shall provide a household member acknowledgment form during onboarding. Client represents that Client has the authority to consent to monitoring on behalf of minor household members. Onboarding and offboarding procedures are governed by Section 7 of the MSA.

4B.5 Personal Data Protections

PTS recognizes the consumer nature of Residential services and commits to the following personal data protections. Additional data protection obligations are set forth in Section 10B of this Agreement (Data Protection Addendum).

- PTS shall not use personal household data for commercial purposes, marketing, data brokerage, sale, or profiling;
- Personal household data is processed only as necessary to deliver Covered Services;
- PTS shall return personal household data within fifteen (15) business days of the effective date of termination of the Residential SOW, per Section 7.6, and shall securely destroy remaining copies within sixty (60) days of termination, unless a longer retention period is required by applicable law;
- PTS shall not share personal household data with third parties except as necessary to deliver Covered Services (e.g., security tool vendors) or as required by law;
- Monitoring data collected from household devices is used only for security monitoring and service delivery purposes.

4B.6 Business Use Prohibited

Covered services under the Guardian Residential tier are for personal and household use only. Client shall not use Residential-tier covered devices or services for:

- Operating a business or commercial enterprise;
- Storing, processing, or transmitting regulated data (HIPAA, GLBA, PCI DSS, or similar);
- Conducting commercial transactions or providing services to third parties;
- Any activity that would subject the covered devices or services to commercial regulatory requirements.

If a household device is used for commercial activities or regulated data, Client must promptly notify PTS. PTS may require Client to upgrade to the appropriate commercial Guardian Tier (Fundamentals or higher). Continued use of Residential services for commercial purposes after notice constitutes a material breach of this Agreement.

4B.7 Minor Data Protections

PTS is committed to protecting the personal data of minor household members. The following protections apply to data collected from or about household members under the age of eighteen (18):

- PTS shall not knowingly collect, use, retain, or disclose personal data of minor household members for any purpose other than service delivery to Client's household;
- PTS shall not use data about minor household members for analytics, profiling, marketing, or any commercial purpose;
- Monitoring data collected from devices used by minor household members is used solely for security and service delivery purposes;
- Client represents that Client has the authority and legal capacity to consent to monitoring and data processing on behalf of minor household members;
- PTS shall delete personal data of minor household members upon Client's request or upon termination of the Residential SOW, consistent with Section 4B.5.

4B.8 Consumer Protection

To the extent that Indiana consumer protection law (including the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 et seq., and the Indiana Consumer Data Protection Act) applies to the Residential services provided hereunder, Client retains all rights afforded by applicable statute. Nothing in this Agreement or this section is intended to limit, waive, or override any statutory consumer protection rights that cannot be waived under applicable Indiana law.

The following table summarizes key consumer rights and disclosures applicable to Guardian Residential clients:

Consumer Right / Disclosure	Summary
Right to Cancel	Residential clients may terminate with 30 days' written notice (shorter than commercial MSA termination provision in Section 13.7, which is overridden for Residential clients by Section 4B.9). Early Termination Fee: the lesser of (a) remaining fees in current term, or (b) one (1) month of recurring fees.
Data Protection	PTS does not sell, share, or use personal household data for commercial, marketing, or data brokerage purposes. See Section 4B.5.
Consumer Protection Laws	Client retains all rights under Indiana Deceptive Consumer Sales Act (IC § 24-5-0.5 et seq.) and Indiana Consumer Data Protection Act. Nothing in this section waives non-waivable statutory rights.

Consumer Right / Disclosure	Summary
Minor Data Protections	PTS does not knowingly collect, use, or retain personal data of minor household members for any purpose other than service delivery. See Section 4B.7.
Monitoring Disclosure	All household members aged 18+ must acknowledge PTS's monitoring policies. Client is responsible for obtaining acknowledgment from household members.
Liability Cap	PTS's liability for Residential services is capped at the lesser of two months' recurring fees or $10,000, per Section 16 of the MSA.
Business Use Prohibition	Guardian Residential is for personal and household use only. Commercial or regulated-data use constitutes a material breach.

4B.9 Right to Cancel — Overrides Section 13.7 for Residential Clients

NOTICE: This Section 4B.9 supersedes and overrides Section 13.7 of this Agreement for all Guardian Residential clients. The commercial early termination provisions of Section 13.7 do not apply to Guardian Residential clients; instead, the terms of this Section 4B.9 exclusively govern the early termination rights and fees for Residential clients.

Guardian Residential clients may terminate their Residential SOW by providing thirty (30) days' written notice to PTS. This thirty (30) day notice period is shorter than the ninety (90) day commercial termination provision in Section 13.7 of the MSA, and that ninety-day provision is expressly overridden for Residential clients by this Section 4B.9. If Client terminates prior to the expiration of the then-current term, Client shall pay an Early Termination Fee equal to the lesser of: (a) the total recurring fees remaining in the then-current term, or (b) one (1) month of recurring fees at the then-current rate. The one-month Early Termination Fee cap is a consumer-specific protection that applies exclusively to the Residential tier.

4B.10 Liability Acknowledgment

Client acknowledges and agrees that:

- Household security depends on the behavior of all household members, including actions taken by household members on covered and non-covered devices;
- PTS is not responsible for security incidents caused by household members' actions, including clicking on phishing links, sharing credentials, installing unauthorized software, or connecting non-approved devices to the home network;
- PTS's liability for Residential services is limited as set forth in Section 16 of the MSA (lesser of two months recurring fees or $10,000);
- The limitations of consumer technology and home networking equipment may affect the level of security achievable;
- PTS does not control physical access to the home or household devices.

4B.11 Cross-References

Acceptable use obligations for Residential services are governed by Section 5B of the MSA. Onboarding and offboarding procedures are governed by Section 7 of the MSA. Change management procedures are governed by Section 8 of the MSA. Pricing and fee schedules for Residential services are governed by Section 12 of the MSA. Third-party tool terms applicable to Residential services are governed by Section 11B of the MSA. Data protection obligations are governed by Section 10B of this Agreement. Incident response scope for the Residential tier is governed by Section 9B of the MSA.

4B.12 Survival

The provisions of this Section 4B that by their nature should survive termination or expiration (including Sections 4B.5, 4B.6, 4B.7, and 4B.10) shall survive in accordance with the survival provisions of the MSA. By executing a Statement of Work that references the Guardian Residential tier, Client acknowledges that Client has read, understands, and agrees to the terms and conditions of this Section 4B.

SECTION 5. CLIENT RESPONSIBILITIES

5.1 Environment Disclosure and Accuracy.

Client shall provide PTS with complete, accurate, and current information regarding Client's IT environment, including all hardware, software, network infrastructure, cloud services, users, third-party service providers, security configurations, and known issues or vulnerabilities. Client shall promptly notify PTS of any material changes to the environment, including changes to the number of users, devices, locations, or third-party integrations. Client acknowledges that PTS's ability to deliver services effectively is directly dependent on the accuracy and completeness of information provided by Client, and that inaccurate or incomplete information may result in service gaps, security exposures, or increased costs for which PTS shall not be liable.

5.2 Minimum Standards and Baseline Eligibility.

Client shall maintain its environment in compliance with the Baseline Requirements set forth in Section 5C of this Agreement applicable to Client's Guardian Tier at all times during the term of this Agreement. Failure to meet or maintain Baseline Requirements may result in: (a) service limitations or reduced service quality; (b) adjusted or eliminated liability caps; (c) suspension of services pending remediation; or (d) termination of this Agreement.

5.3 Access, Cooperation, and Decision-Making.

Client shall provide PTS with timely and adequate access to Client's systems, networks, data, facilities (where applicable), and personnel as reasonably necessary for PTS to perform Covered Services. Client shall cooperate with PTS in good faith, respond to PTS requests within a reasonable timeframe, make timely decisions on matters requiring Client input, and provide all approvals necessary for PTS to perform its obligations. Delays caused by Client's failure to provide access, cooperation, information, or timely decisions shall not constitute a breach by PTS.

5.4 Third-Party Vendors and Internal Staff.

Client is solely responsible for managing its relationships with third-party vendors, internet service providers, software licensors, hardware manufacturers, cloud providers, telecommunications carriers, and other service providers unless PTS has expressly assumed such responsibility in the applicable SOW. Client shall ensure that its internal staff, contractors, and authorized users comply with PTS security policies and procedures applicable to the Client's environment. PTS shall not be liable for acts, omissions, failures, or breaches by Client's third-party vendors, internal staff, contractors, or authorized users.

5.5 Cyber Insurance Recommendation.

PTS strongly recommends that Client maintain a cyber liability insurance policy appropriate to Client's risk profile, industry, and Guardian Tier, with coverage limits at or above the following minimums:

- Guardian Residential: PTS recommends that Client obtain a personal cyber liability rider or equivalent coverage appropriate for household risk exposure.
- Guardian Fundamentals: PTS recommends that Client maintain cyber liability insurance with a minimum coverage limit of Five Hundred Thousand Dollars ($500,000).
- Guardian Compliance: PTS recommends that Client maintain cyber liability insurance with a minimum coverage limit of One Million Dollars ($1,000,000).
- Guardian Co-Managed: PTS recommends that Client maintain cyber liability insurance with a minimum coverage limit of One Million Dollars ($1,000,000).

Client's decision not to obtain or maintain adequate cyber insurance shall not affect PTS's limitation of liability under this Agreement, and Client assumes all financial risk of losses that cyber insurance would otherwise cover.

SECTION 5B. ACCEPTABLE USE AND CLIENT CONDUCT POLICY

5B.1 Purpose.

This Section establishes the rules of conduct for all individuals and entities using PTS-managed systems, tools, and services. Violations may result in suspension or termination of services and may trigger indemnification obligations under this Agreement.

5B.2 Scope.

This Acceptable Use Policy ("AUP") applies to all Guardian Tiers and to all persons who access or use PTS-managed systems, tools, and services, including Client's employees, contractors, household members (Residential tier), and authorized users.

5B.3 Prohibited Activities.

Client and its authorized users shall not:

- Use PTS-managed systems for any unlawful purpose or in violation of any applicable law or regulation;
- Transmit, store, or process content that is obscene, defamatory, threatening, harassing, or that constitutes hate speech;
- Use PTS-managed systems to distribute malware, ransomware, viruses, or other malicious code;
- Engage in unauthorized access to systems, networks, or data (including attempting to bypass security controls);
- Use PTS-managed systems for cryptocurrency mining without prior written approval;
- Interfere with, disable, circumvent, or tamper with PTS monitoring, security, or management tools;
- Share, disclose, or misuse PTS credentials, access tokens, or security configurations;
- Install unauthorized software, tools, or remote access solutions on PTS-managed systems;
- Use PTS-managed systems in a manner that degrades performance or availability for other users or PTS clients;
- Misrepresent identity or impersonate another person or entity;
- Engage in abusive, threatening, or harassing conduct toward PTS personnel.

5B.4 Residential Client Conduct.

In addition to the prohibitions in Section 5B.3, Guardian Residential clients acknowledge and agree that: (a) Client is responsible for the conduct and use of covered services by all household members; (b) Client warrants that covered services are for personal and household use only; commercial use of Residential-tier services requires PTS's prior written consent or upgrade to the appropriate commercial tier; and (c) Client is responsible for ensuring all adult household members are aware of and comply with these use restrictions.

5B.5 Consequences of Violation.

Any violation of this AUP may result in: (a) immediate suspension of services without prior notice; (b) termination of this Agreement in accordance with Section 13.6; (c) indemnification obligations under Section 17.2; and (d) PTS reporting the violation to appropriate law enforcement or regulatory authorities where required by law or where PTS determines reporting is warranted to protect PTS, its clients, or third parties.

5B.6 Monitoring.

PTS monitors systems under management for security, compliance, and performance purposes as described in Section 11 of this Agreement. This monitoring is a condition of service under all Guardian Tiers. Client acknowledges and consents to this monitoring on behalf of itself and all authorized users.

SECTION 5C. SECURITY BASELINE REQUIREMENTS AND POLICIES

5C.1 Purpose and Scope

This Section 5C establishes the minimum technical, operational, and security standards ("Baseline Requirements") that Client must maintain as a condition of service delivery under the applicable Guardian Tier. Compliance with Baseline Requirements is a prerequisite for PTS's service delivery obligations and directly affects the liability caps set forth in this Agreement. PTS may update Baseline Requirements from time to time to reflect evolving threats, technology changes, and industry best practices. PTS shall provide reasonable notice of material changes to Baseline Requirements.

5C.2 Baseline Requirements by Guardian Tier

5C.2.1 Universal Baseline (All Tiers)

- Client must provide truthful and complete information about the IT environment;
- Client must permit PTS to install and operate approved monitoring and security tools;
- Client must not intentionally interfere with, disable, or circumvent PTS tools or configurations;
- Client must report known or suspected security incidents to PTS promptly;
- Client must maintain valid licenses for all software in use on covered systems;
- Client must designate an Authorized Approver for communications and decisions.

5C.2.2 Guardian Ad-Hoc Baseline

No additional baseline requirements beyond the Universal Baseline. Client retains full responsibility for all IT systems and security.

5C.2.3 Guardian Residential Baseline

- Home router must be within five (5) years of manufacture date and running current manufacturer firmware;
- Home WiFi must use WPA2 or WPA3 encryption; default manufacturer passwords must be changed;
- PTS-approved endpoint security agent must be installed and operational on all covered devices;
- Cloud backup must be enabled for all covered devices;
- Multi-factor authentication (MFA) must be enabled for email accounts, financial accounts, and cloud platforms;
- No end-of-life consumer operating systems permitted on covered devices (e.g., Windows 10 and earlier, unsupported macOS versions);
- All covered devices must run supported operating system versions with current security updates;
- Covered mobile devices must have screen lock enabled and not be jailbroken or rooted.

5C.2.4 Guardian Fundamentals Baseline

- All Universal Baseline requirements;
- All servers, workstations, and laptops must run supported, vendor-maintained operating systems with current security updates;
- PTS-approved EDR agent installed on all endpoints;
- PTS-approved RMM agent installed on all covered devices;
- Microsoft 365 tenant must be under PTS partner management;
- MFA enabled for all users on Microsoft 365 and all cloud-based business applications;
- Network firewall in place with PTS-approved configuration;
- PTS-managed backup solution deployed for all critical data and systems;

- Administrative access credentials shared with PTS and stored securely;
- No unauthorized third-party remote access tools;
- All end-of-life hardware and software must be replaced or decommissioned within timelines agreed during onboarding;
- Unique user accounts for all personnel (no shared accounts for daily operations).

5C.2.5 Guardian Compliance Baseline

All Fundamentals Baseline Requirements, plus the following:

- Security awareness training completion for all users within ninety (90) days of enrollment and annually thereafter;
- Phishing simulation program active with PTS-managed campaigns;
- Formal security policies in place (PTS assists with development);
- Privileged access management controls for all administrator accounts;
- Vulnerability scanning performed at least quarterly on all internet-facing systems;
- Security event logging and retention for a minimum of twelve (12) months;
- Designated Compliance Owner available for quarterly reviews and incident response;
- All PTS-recommended remediations implemented within agreed timelines;
- Encryption enabled on all endpoints (full-disk encryption);
- Email filtering and anti-phishing controls in place.

5C.2.6 Guardian Co-Managed Baseline

All Fundamentals Baseline Requirements, plus the following:

- Documented role separation between PTS and internal IT;
- Internal IT must follow PTS escalation and change management procedures per Section 8 of this Agreement;
- Internal IT must not make changes to PTS-managed systems without prior coordination;
- Security event logging and retention for a minimum of twelve (12) months;
- Internal IT must participate in monthly security reviews and quarterly governance meetings;
- Change management discipline must be documented and enforced;
- PTS must have administrative access to all security tooling and infrastructure within scope.

5C.3 Compliance Verification

5C.3.1 Baseline Assessment

PTS will conduct a baseline assessment during onboarding per Section 7 of this Agreement to verify Client's compliance with the applicable Baseline Requirements. Non-compliant items will be documented and a remediation plan will be developed.

5C.3.2 Ongoing Compliance

PTS may periodically verify Client's compliance with Baseline Requirements through monitoring, assessment, or audit. PTS may audit Client's environment annually at no cost to Client to verify Section 5C compliance. Client may dispute audit findings within thirty (30) days.

5C.3.3 Non-Compliance Consequences

Client's failure to maintain Baseline Requirements may result in: (a) reduced or suspended services; (b) adjusted liability caps (PTS's liability may be reduced or eliminated for incidents attributable to non-compliance); (c) required remediation as a condition of continued service; or (d) termination in accordance with this Agreement.

5C.4 Updates to Baseline Requirements

PTS may update Baseline Requirements from time to time to reflect changes in the threat landscape, technology, industry best practices, or regulatory requirements. PTS shall provide at least thirty (30) days' written notice of material changes. Client shall implement required changes within the timeline specified by PTS or as mutually agreed.

SECTION 6. SERVICE DELIVERY AND SUPPORT

6.1 Support Hours.

PTS provides support during the hours specified in the applicable SOW and Section 6B of this Agreement (Service Level Targets and Support Terms). Support hours vary by Guardian Tier. PTS-observed holidays are excluded from standard business hours for all tiers.

6.2 Priority Levels and Response Targets.

PTS classifies service requests by severity and responds within the applicable response targets set forth in Section 6B of this Agreement. Response targets are service objectives and are not guarantees of performance. Failure to meet a response target shall not constitute a material breach of this Agreement.

6.3 Maintenance and Downtime.

PTS may schedule maintenance windows for updates, patching, security configuration changes, and platform maintenance. Scheduled maintenance will be communicated to Client in advance using reasonable notice. PTS will use commercially reasonable efforts to schedule maintenance during off-peak hours and to minimize service disruption.

6.4 Remote Service Delivery.

PTS delivers the majority of Covered Services remotely using approved remote access and management tools. Client consents to such remote access as a condition of receiving Covered Services. Remote access is subject to the security controls and consent provisions of Section 11.2 of this Agreement.

6.5 Service Reporting.

PTS provides service reporting to Client at frequencies and in formats appropriate to the Guardian Tier, as further described in the applicable SOW. Reporting may include ticket summaries, security event reports, patch compliance reports, backup status, and tier-specific governance reports.

6.6 Service Requests and Ticketing.

All service requests must be submitted through PTS-approved channels (ticketing system, support email, or support phone number). PTS is not obligated to respond to service requests submitted through unofficial channels. The SLA clock begins when PTS acknowledges receipt of a properly submitted service request.

6.7 Third-Party Coordination.

PTS may coordinate with Client's third-party vendors, ISPs, cloud providers, and software licensors as necessary to deliver Covered Services. Such coordination is performed as a courtesy and does not make PTS responsible for the performance, failures, or decisions of third parties. PTS's obligations are limited to those expressly included in the applicable SOW.

SECTION 6B. SERVICE LEVEL TARGETS AND SUPPORT TERMS

6B.1 Purpose and Scope

This Section 6B defines the service level targets, support hours, severity classifications, and response targets applicable to each Guardian Tier. These targets are service objectives and are not guarantees of performance. Failure to meet a response target shall not constitute a material breach of this Agreement.

6B.2 Support Hours by Guardian Tier

Guardian Tier	Support Hours	After-Hours Availability
Ad-Hoc	By appointment only; no guaranteed availability	Not available
Residential	Standard business hours (M–F, PTS-defined hours)	Not available unless separately contracted in SOW
Fundamentals	Standard business hours (M–F, hours defined in SOW)	Emergency-only; subject to after-hours fees per SOW
Compliance	Extended business hours as defined in SOW	Available for security incidents as specified in SOW
Co-Managed	As defined in SOW (aligned with client IT schedule)	As defined in SOW

PTS-observed holidays are excluded from standard business hours for all tiers. A list of PTS-observed holidays will be provided during onboarding and updated annually.

6B.3 Severity Classifications

Severity Level	Definition	Examples
Severity 1 (Critical)	Complete loss of a critical business system or confirmed active security breach affecting production systems	Server down; ransomware active; email system completely offline; confirmed data breach in progress
Severity 2 (High)	Significant degradation of a critical system or security incident requiring urgent attention; business operations materially impaired	Intermittent outages; suspected malware on multiple endpoints; backup failure on critical systems; M365 service significantly degraded
Severity 3 (Medium)	Non-critical system issue or minor service degradation; business operations continue with workaround available	Single user unable to access email; printer offline; software installation request; minor network slowness
Severity 4 (Low)	Informational request, planned task, or enhancement with no immediate business impact	New user setup (scheduled); documentation request; how-to question; software upgrade planning

PTS reserves the right to reclassify severity levels based on actual impact assessment. Client may request reclassification, which PTS will evaluate in good faith.

6B.4 Response Targets by Guardian Tier

The following table sets forth the target initial response times for each severity level and Guardian Tier. Response time is measured from the time PTS acknowledges receipt of the service request.

Severity	Ad-Hoc	Residential	Fundamentals	Compliance	Co-Managed
Sev 1 (Critical)	Best effort / T&M	Next business day	4 business hours	2 business hours	2 business hours
Sev 2 (High)	Best effort	2 business days	8 business hours	4 business hours	4 business hours
Sev 3 (Medium)	Best effort	5 business days	1 business day	1 business day	1 business day
Sev 4 (Low)	Best effort	Best effort	Best effort	Best effort	Best effort

6B.5 SLA Clock and Measurement

6B.5.1 SLA Clock Start

The SLA response clock starts when PTS acknowledges receipt of a properly submitted service request through PTS-approved channels (ticketing system, support email, or support phone number).

6B.5.2 SLA Clock Pause

The SLA response clock pauses when PTS is waiting for: (a) Client action, information, or decision required to proceed; (b) Client approval for proposed changes or expenditures; (c) Third-party vendor response, action, or resolution (where the third party is outside PTS's control); (d) Client-scheduled maintenance windows or access periods; or (e) Force Majeure Events. The clock resumes when the blocking condition is resolved. PTS shall document all clock-pause events in the service ticket.

6B.5.3 Residential Tier Support

Residential tier support hours are the same standard business hours as other tiers. There is no after-hours guarantee for Residential clients unless the applicable SOW expressly provides for after-hours support at additional fees. Residential clients may submit requests outside business hours, but response will commence during the next business day.

6B.6 Resolution Targets

PTS does not guarantee specific resolution times. Resolution depends on the nature and complexity of the issue, Client cooperation, third-party dependencies, and availability of replacement parts or vendor support. PTS will use commercially reasonable efforts to resolve issues as expeditiously as possible.

6B.7 Disclaimers

6B.7.1

Response targets are service objectives, not service level guarantees. PTS does not offer financial SLA credits, service credits, or other penalties for failure to meet response targets.

6B.7.2

Response targets do not apply to Out-of-Scope Services, unsupported systems, or issues caused by Client's failure to maintain Baseline Requirements.

6B.7.3

No SLA applies to security outcomes. PTS does not guarantee prevention of security breaches, regardless of the response target tier.

6B.7.4

After-hours support, where available, may be subject to additional fees as specified in the SOW.

6B.8 Escalation Procedures

If Client believes a service request is not receiving appropriate attention, Client may escalate the request by contacting PTS management through the escalation procedures provided during onboarding. Escalation does not change the severity classification but ensures management review.

SECTION 7. ONBOARDING, TRANSITION, AND ACCEPTANCE

7.1 Baseline Assessment.

Upon execution of an SOW, PTS will conduct a baseline assessment of Client's IT environment to document the current state, identify gaps in compliance with applicable Baseline Requirements set forth in Section 5C of this Agreement, and develop a remediation plan. The baseline assessment is a prerequisite to service commencement for all managed Guardian Tiers (Residential, Fundamentals, Compliance, Co-Managed).

7.2 Service Commencement and Acceptance.

Services commence on the date specified in the SOW or, if not specified, upon PTS's written confirmation that onboarding is complete. Client has fifteen (15) business days from service commencement (the "Acceptance Period") to review initial service delivery and notify PTS of any material deficiencies. If Client does not provide written notice of material deficiencies within the Acceptance Period, Client shall be deemed to have accepted the services ("Service Acceptance"). Deemed acceptance does not waive Client's right to raise subsequent service issues through the normal service request process.

7.3 Onboarding Process — General.

The standard onboarding process for managed Guardian Tiers includes the following steps, performed in a sequence appropriate to Client's environment:

- Kickoff Meeting: PTS and Client meet to review the SOW, confirm scope, identify key contacts, and establish the onboarding timeline.
- Information Gathering: Client provides PTS with complete and accurate information about the IT environment per Section 5.1.
- Credential Collection: Client provides PTS with administrative credentials for all covered systems and platforms.
- Network Discovery: PTS performs a network scan and asset discovery to identify covered devices, systems, and configurations.
- Vendor Contact Collection: PTS gathers contact information for third-party vendors, ISPs, and other service providers.
- Discovery and Baseline Assessment: PTS documents the current state of the environment and assesses compliance with applicable Baseline Requirements.
- Remediation Planning: Non-compliant items are documented, and a remediation plan with timelines is agreed between the parties.
- Tool Deployment: PTS deploys monitoring agents, security tools, RMM software, and backup agents on covered devices.
- Configuration and Hardening: PTS applies security configurations, hardening settings, and policy configurations to covered systems.
- Documentation: PTS creates or updates asset inventory, network documentation, and configuration records.
- Acceptance: Client reviews and accepts the onboarded environment per Section 7.2.

7.4 Tier-Specific Onboarding.

7.4.1 Ad-Hoc Onboarding.

Ad-Hoc engagements do not require a formal onboarding process. Each engagement is initiated by execution of an applicable SOW or Order Form. No baseline assessment is required unless specified in the SOW. No tool deployment is required.

7.4.2 Residential Onboarding.

Residential onboarding includes the following additional elements:

- Household assessment: PTS inventories all devices to be covered and identifies household composition;
- Resident acknowledgment: All adult household members (18+) sign the monitoring acknowledgment form;
- Residential Terms: Client acknowledges Section 4B of this Agreement (Residential Terms);
- Home network review: PTS reviews home router configuration and WiFi settings for compliance with Section 5C.2.3 of this Agreement;
- Device enrollment: PTS enrolls all covered devices in the monitoring and management platform;
- Baseline verification: PTS verifies that all covered devices meet the Residential Baseline requirements in Section 5C.2.3 of this Agreement.

7.4.3 Fundamentals Onboarding.

Fundamentals onboarding follows the General Onboarding Process in Section 7.3, with particular emphasis on: (a) Microsoft 365 tenant transfer to PTS partner management; (b) deployment of all five required sub-component tool stacks; (c) firewall configuration review and hardening; and (d) backup agent deployment and initial backup verification.

7.4.4 Compliance Onboarding.

Compliance onboarding includes all Fundamentals onboarding elements, plus: (a) initial security risk assessment; (b) compliance framework gap analysis (CIS Controls / NIST CSF); (c) designation and introduction of Compliance Owner; (d) security policy review and initial policy development plan; (e) enrollment in security awareness training platform; (f) SIEM and logging configuration; and (g) initial tabletop exercise scheduling.

7.4.5 Co-Managed Onboarding.

Co-Managed onboarding includes development and execution of the Shared Responsibility Matrix, defining PTS-owned, client-owned, and shared responsibilities. Co-Managed onboarding also includes integration with the client's existing IT processes, documentation of escalation procedures, and initial joint security review.

7.5 Transition-Out and Offboarding.

Upon termination or expiration of this Agreement or any SOW, PTS will provide transition assistance for a period of up to thirty (30) days (the "Transition Period") to facilitate an orderly handoff of services, data, and documentation. During the Transition Period, Client continues to pay all applicable fees.

7.6 General Offboarding Process.

The standard offboarding process includes:

- Transition Planning: PTS and Client develop a transition plan within five (5) business days of notice of termination.
- Data Return: PTS provides Client Data in a commercially standard format within fifteen (15) business days of the effective date of termination.
- Tool Removal: PTS removes its agents, tools, and software from covered devices upon expiration of the Transition Period.
- Credential Transfer: PTS transfers all Client-owned credentials, licenses, and account access to Client or Client's designated successor.
- Vendor Transition: PTS cooperates with Client's incoming service provider, subject to confidentiality obligations.
- Access Revocation: PTS revokes all access to Client's systems upon completion of offboarding.

- Final Documentation: PTS provides final documentation package to Client.

7.7 Residential Offboarding.

Residential offboarding includes removal of PTS tools from all covered devices, return of any device access credentials, and a final security summary report. PTS will provide remote offboarding assistance. On-site offboarding is available at T&M rates if requested.

SECTION 8. CHANGE MANAGEMENT

8.1 Change Classifications.

PTS classifies changes to the Client environment into three categories:

- Standard Change: A pre-approved, low-risk, routine change performed in accordance with established procedures. Standard Changes do not require individual approval from the Client's Authorized Approver and may be implemented by PTS during normal business hours without advance notice. Examples include: routine patch deployment, antivirus signature updates, approved tool updates, and pre-authorized configuration changes within established parameters.
- Normal Change: A change that requires review, planning, and Client approval before implementation. Normal Changes are scheduled in advance and implemented during agreed maintenance windows. Examples include: new software deployment, firewall rule modifications, M365 policy changes, user permission changes, and infrastructure upgrades.
- Emergency Change: A change that must be implemented immediately to restore service, prevent imminent security compromise, or address a critical system failure. Emergency Changes may be implemented without advance approval where delay would cause material harm, subject to the notification requirements of Section 8.2.

8.2 Change Authorization.

Normal Changes require written approval from Client's Authorized Approver before implementation. PTS will submit a change request through the agreed change management process, describing the proposed change, scope, risk, rollback plan, and implementation schedule. Client shall respond to change requests within three (3) business days. Emergency Changes may be implemented without prior approval if delay would cause material harm, provided that PTS notifies Client as soon as practicable (and in any event within twenty-four (24) hours) and obtains retroactive approval within five (5) business days.

8.3 Deemed Approval.

If Client fails to approve or reject a Normal Change request within five (5) business days after the due date for response, PTS may treat the change as approved (deemed approval) and proceed with implementation, unless Client has communicated a specific objection or has requested additional information. Deemed approval does not apply to changes that would materially expand the scope or cost of services beyond the applicable SOW.

8.4 Change Documentation.

PTS maintains a change log documenting all Normal Changes and Emergency Changes implemented in Client's environment, including the date, description, approver, and outcome. Change logs are available to Client upon request.

8.5 Tier-Specific Change Management.

8.5.1 Ad-Hoc.

Change management does not apply to the Ad-Hoc tier. Each service request is authorized individually as described in the applicable SOW or Order Form. PTS will seek Client authorization before commencing any work.

8.5.2 Residential.

For Guardian Residential clients, Standard Changes (routine maintenance, patches, security updates) are performed without advance notice. Significant changes to the home network configuration, software, or covered devices require Client notification and approval before implementation. PTS will communicate planned changes to Residential clients in plain, non-technical language.

8.5.3 Fundamentals.

All three change categories apply at the Fundamentals tier. Standard Changes are documented but do not require individual approval. Normal Changes require Authorized Approver sign-off. Emergency Changes may be implemented immediately with retroactive notification and approval. PTS maintains a formal change log for all Fundamentals clients.

8.5.4 Compliance.

Compliance tier change management includes enhanced controls: all Normal Changes are logged with compliance-relevant metadata; Emergency Changes trigger a formal incident-adjacent review process; all changes are recorded in the SIEM for audit trail purposes. The Compliance Owner must be notified of all Normal and Emergency Changes.

8.5.5 Co-Managed.

Co-Managed change management requires coordination between PTS and the client's internal IT team as defined in the Shared Responsibility Matrix. Changes to PTS-managed systems require PTS involvement; changes to client-managed systems require client IT initiation with PTS notification. PTS and client IT hold a monthly change review meeting.

8.6 Unauthorized Changes.

If Client's internal staff, contractors, or authorized users make unauthorized changes to PTS-managed systems or configurations without PTS coordination, PTS may: (a) suspend affected services pending investigation and remediation; (b) bill Client for the time and materials required to remediate the unauthorized changes; and (c) adjust or eliminate applicable liability caps for any issues caused by or related to the unauthorized changes. Repeated unauthorized changes may constitute a basis for termination under Section 13.6.

SECTION 9. SECURITY, INCIDENTS, AND RISK ALLOCATION

9.1 Shared Responsibility Model.

PTS and Client share responsibility for information security. The allocation of security responsibilities depends on the Guardian Tier and is detailed in Section 3B of this Agreement and the applicable SOW. At all tiers, Client retains certain baseline security obligations that cannot be delegated to PTS, including: maintaining accurate information about the environment; not interfering with PTS security tools; training and managing personnel; reporting suspected incidents promptly; and maintaining the IT environment in compliance with Baseline Requirements.

At higher Guardian Tiers, PTS assumes a more active role in security operations, governance, and incident response. Notwithstanding any other provision of this Agreement, PTS's security obligations are limited to the specific services included in the applicable SOW and Guardian Tier. PTS is not responsible for security failures attributable to Client's failure to fulfill its security obligations.

9.2 Security Incidents and Notification.

Upon detecting or receiving notification of a confirmed Security Event affecting Client's Covered Assets or Client Data, PTS will:

- Initiate the incident response process appropriate to Client's Guardian Tier (as described in Section 9B of this Agreement);
- Notify Client's designated incident response contact as soon as reasonably practicable, and within the notification target applicable to Client's Guardian Tier;
- For Guardian Compliance clients: use commercially reasonable efforts to notify Client within seventy-two (72) hours of confirming a Security Event (the "72-Hour Notification Target"). This notification target is a service objective and is not a guarantee. Notification may be delayed if PTS determines that premature notification would interfere with containment, law enforcement investigation, or evidence preservation.

Client is solely responsible for determining and fulfilling any regulatory notification obligations arising from Security Events, including notifications to regulatory agencies, affected individuals, business partners, or insurers. PTS may assist with regulatory notification as an Out-of-Scope Service at additional fees.

9.3 Incident Response Scope.

The scope of PTS's incident response obligations by Guardian Tier is set forth in Section 9B of this Agreement. Extended incident response beyond the included scope is available as an Out-of-Scope Service at applicable time-and-materials or project rates.

9.4 Residual Risk Acknowledgment.

Client acknowledges and accepts that:

- No security technology, managed service, or combination thereof can eliminate all cybersecurity risk;
- Despite PTS's commercially reasonable efforts, Security Events may occur even when PTS has fully performed its obligations under this Agreement;
- The risk of ransomware, data breaches, business email compromise, social engineering attacks, and supply chain compromises cannot be fully mitigated;
- PTS's liability for Security Events is limited as set forth in Section 16 of this Agreement and Section 16.2 of this Agreement;
- Maintaining cyber liability insurance is Client's primary risk transfer mechanism for cybersecurity losses beyond PTS's liability caps.

9.5 Security Recommendations.

PTS may issue security recommendations to Client from time to time, including recommendations for software updates, configuration changes, policy implementations, user training, and additional security controls. Client is strongly encouraged to implement security recommendations promptly. PTS's liability for any Security Event shall be reduced proportionally to the extent that the Security Event was caused or exacerbated by Client's failure to implement a security recommendation made by PTS within a reasonable timeframe.

9.6 Security Tools and Updates.

PTS may update, modify, or replace security tools deployed in Client's environment from time to time to maintain effectiveness against evolving threats. PTS shall provide reasonable notice of material tool changes. Client must permit such updates and must not interfere with or disable updated tools.

9.7 Client Security Testing.

Client shall not conduct penetration testing, vulnerability scanning, red team exercises, or similar security testing on systems managed or shared with PTS without PTS's prior written approval. Unauthorized testing may be misidentified as an attack and may trigger incident response procedures at Client's cost. PTS-approved testing shall be conducted pursuant to a written testing agreement that specifies scope, timing, and rules of engagement.

SECTION 9B. INCIDENT RESPONSE SCOPE AND FEES

9B.1 Purpose and Scope

This Section 9B defines the scope of PTS's incident response ("IR") obligations by Guardian Tier, identifies services included in the recurring fees versus those billed separately, and establishes the framework for extended incident response engagements.

9B.2 Incident Response by Guardian Tier

Guardian Tier	Included IR Scope	Extended Response	Forensics
Ad-Hoc	No IR included; all IR services are billable on a T&M basis	T&M only	Not included; available as separate engagement
Residential	Basic advisory only (guidance on containment and next steps); no hands-on forensics	Extended response billable at T&M rates	Not included; available as separate engagement
Fundamentals	Initial triage and advisory; basic containment guidance; alert review	All extended response beyond initial triage billed separately at T&M or project rates	Not included; available as separate engagement
Compliance	Coordinated IR response; post-incident reporting; Compliance Owner engagement	Forensics and regulatory notification excluded unless separately contracted	Available as separate engagement; PTS coordinates with third-party forensic providers
Co-Managed	Coordinated response within the shared-responsibility model; PTS responds within PTS-managed scope	Client internal IT responsible for client-controlled systems; extended PTS response billable	Available as separate engagement

9B.3 Compliance Tier — 72-Hour Notification Target

For Guardian Compliance clients, PTS shall use commercially reasonable efforts to notify Client within seventy-two (72) hours of confirming a Security Event affecting Client Data or Covered Assets. This 72-Hour Notification

Target is a service objective, not a guarantee, and is subject to the exceptions set forth in Section 9.2 of this Agreement.

9B.4 Incident Response Process

9B.4.1 Detection and Triage

PTS monitors Covered Assets using approved tools and responds to alerts based on the severity classifications in Section 6B of this Agreement. Upon detecting a potential Security Event, PTS performs initial triage to assess scope, severity, and impact.

9B.4.2 Containment

Where authorized and within the scope of Covered Services, PTS takes reasonable containment measures to limit the spread and impact of a confirmed Security Event. Containment may include isolating affected systems, disabling compromised accounts, or implementing emergency firewall rules.

9B.4.3 Client Notification

PTS notifies Client of confirmed Security Events in accordance with Section 9.2 of this Agreement and the notification targets applicable to Client's Guardian Tier.

9B.4.4 Remediation and Recovery

PTS assists with remediation and recovery within the scope of Covered Services. Extended remediation beyond the included scope is billed separately at the rates specified in the SOW or PTS's then-current rate card.

9B.4.5 Post-Incident Reporting

For Compliance and Co-Managed clients, PTS provides a post-incident report documenting the timeline, scope, containment actions, root cause (if determinable), and recommended remediation steps.

9B.5 Exclusions

The following are excluded from PTS's incident response obligations under all tiers unless separately contracted:

- Forensic investigation and evidence preservation for legal or regulatory proceedings;
- Regulatory notification on behalf of Client (Client retains responsibility);
- Public relations, media response, or crisis communications;
- Litigation support or expert witness services;
- Ransom negotiation or ransom payment;
- Data recovery from failed or encrypted media not covered by PTS-managed backup;
- Incident response for systems, devices, or networks not identified as Covered Assets.

9B.6 Extended Incident Response Engagements

If an incident requires response beyond the included scope, PTS will provide a scope and fee estimate for Client approval before commencing extended work. Emergency situations may require PTS to begin work before formal approval, in which case PTS will seek approval as soon as practicable.

9B.7 Client Obligations During Incidents

- Cooperate with PTS during investigation and response;
- Provide timely access to affected systems and personnel;
- Refrain from actions that may compromise evidence or exacerbate the incident;
- Designate a single point of contact for incident communications;
- For Compliance clients: ensure the designated Compliance Owner is available and responsive.

SECTION 10. DATA PROTECTION AND CONFIDENTIALITY

10.1 Confidential Information.

Each party (the "Receiving Party") agrees to: (a) hold the other party's Confidential Information in strict confidence; (b) use Confidential Information solely for the purpose of performing its obligations or exercising its rights under this Agreement; (c) not disclose Confidential Information to any third party without the disclosing party's prior written consent, except as permitted herein; and (d) protect Confidential Information with at least the same degree of care it uses to protect its own confidential information, but in no event less than reasonable care.

The obligations of this Section do not apply to information that: (a) was or becomes publicly available through no breach by the Receiving Party; (b) was rightfully known to the Receiving Party without restriction prior to disclosure; (c) is rightfully obtained from a third party without restriction; or (d) is independently developed by the Receiving Party without use of or reference to the disclosing party's Confidential Information. The Receiving Party may disclose Confidential Information as required by applicable law, regulation, or court order, provided that the Receiving Party: (i) provides prompt prior written notice to the disclosing party (to the extent legally permitted); (ii) cooperates with the disclosing party in seeking a protective order or other appropriate relief; and (iii) discloses only the minimum information required.

Each party's confidentiality obligations shall continue for three (3) years following termination or expiration of this Agreement, except that: (a) trade secrets shall be protected for as long as they qualify as trade secrets under applicable law; and (b) all obligations relating to Client Data shall survive termination indefinitely until all Client Data has been returned or destroyed.

10.2 Data Handling and Retention.

PTS processes Client Data solely as necessary to provide Covered Services. PTS shall not sell, rent, or commercially exploit Client Data. PTS shall implement and maintain appropriate technical, administrative, and organizational security measures to protect Client Data against unauthorized access, use, disclosure, alteration, or destruction. PTS shall retain Client Data for the period necessary to perform Covered Services and, upon termination or expiration of this Agreement, shall return Client Data within fifteen (15) business days of the effective date of termination, per Section 7.6, and shall securely destroy all remaining copies within sixty (60) days of the effective date of termination, unless a longer retention period is required by applicable law.

10.3 Residential Data.

For Guardian Residential clients, Client Data includes personal data relating to household members, including minors who use covered devices. PTS shall handle residential personal data in accordance with applicable consumer privacy laws, including the Indiana Consumer Data Protection Act. PTS's specific data handling practices for Residential clients are set forth in the applicable Privacy Notice provided to Residential clients at or before enrollment.

10.4 Regulatory Alignment.

Where Client is subject to specific data protection regulations (e.g., HIPAA, GLBA, CCPA, GDPR), the handling of regulated data is addressed in the applicable sections of this Agreement: Section 10B (Data Protection Addendum) applies to all commercial tiers processing Personal Data; Section 10C (Healthcare and HIPAA Services) applies to HIPAA-covered entities; Section 11C (AI Services) addresses AI data use. All applicable terms are contained within this Agreement.

SECTION 10B. DATA PROTECTION ADDENDUM

APPLICABILITY: This Section 10B sets forth PTS's data protection obligations applicable to all Guardian Tiers. This section constitutes a Data Processing Agreement under applicable data protection laws, including GDPR Article 28 where applicable.

10B.1 Purpose and Scope

This Data Protection Addendum ("DPA") supplements the MSA and governs the processing of Client Data, including Personal Data, by PTS in the course of providing Covered Services. This section applies to all Guardian Tiers.

10B.2 Definitions

For purposes of this section, the following terms have the meanings set forth below, in addition to the definitions in Section 3 of the MSA:

- "Data Controller" means the party that determines the purposes and means of the processing of Personal Data.
- "Data Processor" means the party that processes Personal Data on behalf of the Data Controller.
- "Processing" means any operation or set of operations performed on Personal Data, including collection, recording, organization, storage, adaptation, retrieval, use, disclosure, and deletion.
- "Sub-Processor" means a third party engaged by PTS to process Personal Data on PTS's behalf.
- "Personal Data" means any information relating to an identified or identifiable natural person, as defined under applicable data protection law.
- "Data Subject" means the identified or identifiable natural person to whom Personal Data relates.

10B.3 Roles and Responsibilities

Client is the Data Controller for Client Data and Personal Data processed in connection with Covered Services. PTS is the Data Processor, processing Personal Data only on Client's instructions as set forth in this Agreement and the applicable SOW. PTS shall not process Personal Data for any purpose other than delivering Covered Services unless required by applicable law.

10B.4 Data Processing Principles

- PTS shall process Personal Data only as necessary to perform Covered Services and as instructed by Client;
- PTS shall implement and maintain commercially reasonable technical and organizational measures to protect Personal Data;
- PTS shall ensure that personnel authorized to process Personal Data are bound by confidentiality obligations;
- PTS shall assist Client, at Client's cost, in responding to data subject requests and regulatory inquiries to the extent reasonably feasible;
- PTS shall notify Client without undue delay upon becoming aware of a Personal Data breach.

10B.5 GDPR Article 28 Provisions

To the extent Client is subject to the General Data Protection Regulation (EU) 2016/679 ("GDPR") or the UK GDPR, this Section 10B.5 constitutes the data processing agreement required by GDPR Article 28. PTS shall, in its capacity as Data Processor:

- Process Personal Data only on documented instructions from Client, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law;
- Ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Implement appropriate technical and organizational measures as set forth in Section 10B.11 (Security Measures) of this Agreement;
- Respect the conditions for engaging another processor (Sub-Processor) as set forth in Section 10B.6 (Sub-Processors);
- Taking into account the nature of the processing, assist Client by appropriate technical and organizational measures in fulfilling Client's obligation to respond to requests for exercising data subjects' rights under Chapter III of the GDPR;
- Assist Client in ensuring compliance with GDPR Articles 32 through 36 (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to PTS;
- At Client's choice, delete or return all Personal Data to Client after the end of the provision of services relating to processing, and delete existing copies unless applicable law requires storage of the Personal Data;
- Make available to Client all information necessary to demonstrate compliance with GDPR Article 28 obligations and allow for and contribute to audits, including inspections, conducted by Client or another auditor mandated by Client, subject to the audit procedures in Section 10B.10.

PTS shall immediately inform Client if, in PTS's opinion, an instruction from Client infringes the GDPR or other applicable EU or Member State data protection provisions.

10B.6 Sub-Processors

PTS may engage Sub-Processors to assist in delivering Covered Services. PTS shall maintain a list of current Sub-Processors and shall notify Client of any material changes. PTS shall ensure that Sub-Processors are bound by data protection obligations no less protective than those in this section. Client may object to a new Sub-Processor within fifteen (15) days of notification; if PTS cannot reasonably accommodate the objection, Client may terminate the affected SOW.

Sub-processor register (updated September 28, 2026). Vendors are current unless expressly marked prospective. Listing a prospective vendor does not mean Client Data is currently processed by that vendor or that a migration has been authorized. Before activation, PTS will confirm processing locations and safeguards and follow the notice and objection process in Section 10B.6 and any applicable stack-change notice under Section 11B.3.

Sub-Processor	Purpose	Location	Safeguard
Microsoft Corporation	Cloud infrastructure, Microsoft 365, Azure, and Entra ID	United States	Microsoft Products and Services Data Protection Addendum
NinjaOne, LLC	Remote monitoring and management, endpoint management, and endpoint and server backup	United States	NinjaOne DPA
Halo Service Solutions Ltd (HaloPSA)	Service desk ticketing, contract, and asset records	United Kingdom (provider); hosted in United States region	Halo DPA; standard contractual clauses or UK transfer addendum where applicable
SentinelOne, Inc.	Endpoint detection and response (EDR)	United States	SentinelOne DPA

Sub-Processor	Purpose	Location	Safeguard
Blackpoint Cyber	Managed detection and response (MDR), security operations center, and current SIEM services	United States	Blackpoint DPA
ThreatLocker, Inc.	Application allowlisting and ringfencing	United States	ThreatLocker DPA
Zorus, Inc.	DNS filtering	United States	Zorus DPA
ConnectWise, LLC (ScreenConnect)	Remote access and remote support sessions	United States	ConnectWise DPA
Keeper Security, Inc.	Password management and credential vault	United States	Keeper DPA
Hudu Technologies, Inc.	IT documentation	United States	Hudu DPA
INFIMA Security, Inc.	Security awareness training and phishing simulation	United States	INFIMA DPA
EasyDMARC Inc.	Email authentication (SPF, DKIM, DMARC) monitoring	United States	EasyDMARC DPA
CyberDrain B.V. (CIPP)	Multi-tenant Microsoft 365 and Entra ID administration	Netherlands (provider); hosted in Microsoft Azure	CyberDrain DPA; standard contractual clauses where applicable
CodeTwo sp. z o.o.	Centralized email signature management for Microsoft 365	Poland (provider); hosted in Microsoft Azure, United States region	CodeTwo DPA; standard contractual clauses where applicable
Cytracom, LLC	UCaaS and voice services (only where contracted in the SOW)	United States	Cytracom DPA
Huntress (prospective provider)	Potential SIEM replacement; under evaluation and not currently deployed by PTS	Processing region to be confirmed before deployment	Applicable DPA and transfer safeguards to be confirmed before any Client Data is processed
Additional vendors	As listed in current SOW or PTS vendor disclosure	Varies	Applicable DPA on file

10B.7 CCPA Provisions

To the extent Client is subject to the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), this Section 10B.7 applies. PTS's obligations as a "service provider" or "contractor" under the CCPA are as follows:

- PTS shall not sell or share Personal Information (as defined under the CCPA) of Client's California resident consumers;
- PTS shall not retain, use, or disclose Personal Information for any purpose other than the business purposes specified in this Agreement and the applicable SOW, or as otherwise permitted by the CCPA;
- PTS shall not retain, use, or disclose Personal Information outside of the direct business relationship between PTS and Client;
- PTS certifies that it understands and will comply with the restrictions of this Section and the CCPA;

- PTS shall assist Client in responding to verifiable consumer requests under the CCPA (access, deletion, correction, opt-out) to the extent technically feasible and at Client's cost;
- PTS shall notify Client within five (5) business days of receiving a verifiable consumer request related to Client's Personal Information in PTS's possession.

10B.8 Indiana Consumer Data Protection Act Provisions

To the extent that the Indiana Consumer Data Protection Act (IC 24-15 et seq.) ("ICDPA") applies to the processing of Personal Data under this Agreement, this Section 10B.8 governs PTS's obligations as a "processor" under the ICDPA:

- PTS shall process Personal Data only in accordance with Client's documented instructions and as set forth in this section;
- PTS shall assist Client in fulfilling its obligations under the ICDPA, including responding to consumer rights requests (access, correction, deletion, portability, and opt-out);
- PTS shall make available to Client all information necessary to demonstrate compliance with the ICDPA;
- PTS shall allow for and contribute to audits and inspections conducted by Client or a third party mandated by Client, subject to the audit procedures in Section 10B.10;
- PTS shall engage Sub-Processors only pursuant to a written contract that imposes the same data protection obligations as this section;
- PTS shall notify Client promptly upon determining that PTS can no longer meet its obligations under the ICDPA.

10B.9 Data Retention and Deletion

Upon termination of the Agreement or the applicable SOW, PTS shall return Personal Data within fifteen (15) business days of the effective date of termination, per Section 7.6, and shall securely delete all remaining copies within sixty (60) days of the effective date of termination, unless retention is required by applicable law. PTS may retain anonymized or aggregated data that does not identify any individual.

10B.10 Audit Rights

Client may request, no more than once per year and with at least thirty (30) days' notice, reasonable documentation or evidence of PTS's compliance with this section. PTS may satisfy such requests through third-party audit reports, certifications, or written responses. On-site audits require mutual agreement on scope, timing, and confidentiality protections. For GDPR purposes, the audit right in this Section satisfies the requirement of GDPR Article 28(3)(h).

10B.11 Security Measures

PTS implements and maintains the following technical and organizational security measures to protect Personal Data:

Measure	Description
Encryption at Rest	AES-256 encryption for stored Client Data and Personal Data on PTS-managed systems
Encryption in Transit	TLS 1.2 or higher for all data transmitted over public networks
Access Controls	Role-based access control (RBAC); principle of least privilege; MFA enforced for all PTS personnel accessing Client Data
Logging and Monitoring	Centralized SIEM logging; access logs retained for minimum 90 days; anomaly alerting

Measure	Description
Vulnerability Management	Monthly vulnerability scanning; critical/high patches applied within 30 days; penetration testing annually for Compliance tier
Incident Response	Documented IR plan; security events handled per Section 9B of the MSA
Backup and Recovery	Automated backups per SOW; recovery tested periodically; RPO/RTO per applicable SOW
Personnel Controls	Background checks for personnel with access to Client Data; annual security awareness training; confidentiality obligations
Vendor Management	Sub-Processors assessed for data protection compliance; sub-processor agreements in place
Physical Security	PTS does not operate primary data centers; cloud infrastructure security managed by hyperscale providers (see Sub-Processor list)

10B.12 Data Transfers

PTS processes data primarily within the United States. If Client Data is transferred outside the United States, PTS shall ensure appropriate safeguards are in place consistent with applicable data protection laws. PTS shall notify Client of any material change in the location of data processing. For transfers subject to GDPR, PTS will implement appropriate transfer mechanisms (e.g., Standard Contractual Clauses) as required.

10B.13 Data Subject Rights Procedures

The following table summarizes data subject rights and the parties' respective responsibilities:

Right	Description	Responsibility
Right of Access	Individual requests a copy of their Personal Data held by the controller	Client (Controller) responds; PTS assists upon request at Client's cost
Right to Rectification	Individual requests correction of inaccurate Personal Data	Client handles; PTS updates data in PTS-managed systems upon Client instruction
Right to Erasure / Deletion	Individual requests deletion of Personal Data	Client handles; PTS deletes applicable data in PTS systems within 30 days of Client instruction
Right to Restriction of Processing	Individual requests restriction of processing pending resolution of a dispute	Client handles; PTS restricts processing upon written Client instruction
Right to Data Portability	Individual requests export of Personal Data in machine-readable format	PTS provides export of applicable Client Data upon written request
Right to Object / Opt Out	Individual objects to processing or opts out of sale/sharing (CCPA)	Client handles opt-out; PTS does not sell or share Personal Data
Right to Non-Discrimination (CCPA)	Consumer asserts right not to be discriminated against for exercising CCPA rights	PTS does not discriminate; service terms apply equally

PTS shall respond to Client's request for assistance with data subject rights within ten (10) business days of receipt, unless a shorter period is required by applicable law.

10B.14 Residential Data Protections

For Guardian Residential clients, the following additional protections apply:

- Personal and household data is processed only as necessary to deliver Covered Services to Client and Client's household;
- PTS shall not use household personal data for commercial purposes, marketing, data brokerage, sale, or any purpose unrelated to service delivery;
- Household members' data shall be treated as consumer personal data under applicable state law, including the Indiana Consumer Data Protection Act and any other applicable consumer privacy statute;
- Client is the Data Controller for household data; PTS acts as a Data Processor in a limited capacity, processing household data solely to deliver Covered Services;
- PTS shall return household data within fifteen (15) business days of the effective date of termination, per Section 7.6, and shall securely destroy remaining copies within sixty (60) days of termination, unless a longer retention period is required by applicable law;
- PTS shall not create profiles of household members for purposes unrelated to service delivery;
- Monitoring data collected from household devices shall be used only for security and service delivery purposes.

10B.15 Regulatory Compliance

This section establishes PTS's general data protection obligations. Compliance with specific regulatory frameworks (HIPAA, GLBA, GDPR, CCPA, etc.) requires application of the applicable sections of this Agreement. This section does not create implied compliance obligations beyond its express terms.

Cross-references: Acceptable use obligations are governed by Section 5B of the MSA. Onboarding and offboarding procedures are governed by Section 7 of the MSA. Change management procedures are governed by Section 8 of the MSA. Pricing and fee schedules are governed by Section 12 of the MSA. Third-party and vendor terms are governed by Section 11B of the MSA. Healthcare and HIPAA services are addressed in Section 10C of this Agreement. AI services data use is addressed in Section 11C of this Agreement.

SECTION 10C. HEALTHCARE AND HIPAA SERVICES

APPLICABILITY: This Section 10C applies only where Client is a covered entity or business associate under HIPAA and the applicable SOW involves services that may implicate Protected Health Information. This section is not applicable to clients for whom no SOW involves PHI.

This Section 10C sets forth PTS's healthcare and HIPAA service obligations. This section governs the provision of IT and security services to Client where Client is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations (collectively, "HIPAA Rules").

10C.1 Purpose and Scope

This Healthcare and HIPAA Services section supplements the MSA and governs the provision of IT and security services to Client where Client is subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations (collectively, "HIPAA Rules"). This Section 10C applies only where Client is a covered entity or business associate under HIPAA and where the applicable SOW involves services that may implicate Protected Health Information ("PHI").

10C.2 Minimum Tier Requirement

This section requires enrollment in Guardian Compliance as the minimum tier. Guardian Co-Managed clients may apply this section with a signed risk acceptance acknowledging the shared responsibility model and the

limitations of shared control over protected health information (PHI). This section is not available at the Ad-Hoc, Residential, or Fundamentals tiers.

10C.3 Business Associate Relationship

To the extent PTS creates, receives, maintains, or transmits Protected Health Information (PHI) on behalf of Client in the course of providing Covered Services, PTS is a Business Associate as defined under HIPAA Rules. The parties shall execute a separate Business Associate Agreement ("BAA") as required by 45 C.F.R. § 164.502(e). The BAA shall govern the parties' obligations with respect to PHI and shall be incorporated into this Agreement by reference.

No PHI shall be disclosed to PTS, and PTS shall not access, receive, or process any PHI, until a fully executed BAA is in place between the parties. Disclosure of PHI to PTS without an executed BAA constitutes a material breach of this Agreement.

10C.4 PTS Obligations

In connection with the provision of HIPAA-related services under this section, PTS shall:

- Implement administrative, physical, and technical safeguards consistent with the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) with respect to PHI in PTS's possession or control;
- Report security incidents involving PHI to Client as required by the BAA and HIPAA Breach Notification Rule (45 C.F.R. Part 164, Subpart D), and per the incident response procedures in Section 9B of the MSA;
- Ensure that PTS personnel with access to PHI receive appropriate HIPAA training on an annual basis and prior to accessing PHI;
- Support Client's compliance with the HIPAA Security Rule through security control mapping, risk assessment support, and remediation guidance within the scope of Covered Services;
- Maintain audit logs and access records for PHI in PTS-managed systems as required by the BAA;
- Cooperate with Client's HIPAA compliance officer and legal counsel as reasonably required;
- Ensure that any sub-processors or subcontractors who receive, access, or process PHI execute a Business Associate Agreement with PTS on terms no less protective than the BAA between Client and PTS;
- Not use or disclose PHI except as permitted or required by the BAA and applicable HIPAA Rules.

10C.5 Client Obligations

In connection with the provision of HIPAA-related services under this section, Client shall:

- Execute a BAA with PTS before disclosing or permitting access to PHI;
- Identify all systems, devices, and workflows that involve PHI and provide PTS with a current inventory prior to commencement of HIPAA-related services;
- Designate a HIPAA Compliance Officer (may be combined with the Compliance Owner role under the MSA);
- Implement and maintain all client-side HIPAA requirements, including workforce training, physical safeguards, and policies and procedures;
- Notify PTS immediately — and in no event later than twenty-four (24) hours — of any known or suspected unauthorized access to PHI;
- Comply with all applicable HIPAA Rules and applicable state health information privacy laws;
- Not disclose PHI to PTS beyond what is minimally necessary to accomplish the intended purpose of the Covered Services.

10C.6 HIPAA Safeguard Responsibilities

Safeguard Category	Requirement	Responsibility
Administrative Safeguards	Documented security management process; designated security official; workforce security training; contingency plan; periodic evaluation	Both parties — Client maintains internal policies; PTS maintains PTS-side policies and supports Client's compliance
Physical Safeguards	Facility access controls; workstation use policies; device and media controls	Client responsible for client-side physical controls; PTS cloud infrastructure managed by sub-processors (see Section 10B.6)
Technical Safeguards	Access controls; audit controls; integrity controls; transmission security (TLS 1.2+)	PTS implements on PTS-managed systems; Client implements on client-controlled systems
Breach Notification	Notification of breach of unsecured PHI to Client; Client notifies HHS and affected individuals as required by HIPAA Breach Notification Rule	PTS notifies Client per Section 9B of the MSA and BAA; Client handles regulatory notifications
Business Associate Agreement	Executed BAA required before any PHI is disclosed to PTS; governs PHI handling, permitted uses, sub-contractor obligations	Parties execute BAA separately; BAA incorporated into Agreement by reference
Access to PHI	Access to PHI limited to workforce members with a need-to-know; RBAC enforced; access logs maintained	PTS enforces on PTS-managed systems; Client enforces on client-controlled systems
Minimum Necessary Standard	PHI accessed, used, or disclosed only to the minimum extent necessary to accomplish the intended purpose	Both parties observe minimum necessary standard

10C.7 HITECH Provisions

To the extent applicable, PTS's obligations under this section incorporate the requirements of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), including:

- The enhanced breach notification requirements under HITECH Section 13402, which require notification to affected individuals, HHS, and (for breaches affecting 500 or more residents of a state) prominent media outlets; Client is responsible for such notifications, with PTS providing support as set forth in the BAA;
- The prohibition on use or disclosure of PHI for marketing or sale of PHI without authorization, consistent with HITECH Section 13405;
- The obligation to honor restrictions on disclosures of PHI where Client has agreed to such restrictions under HITECH Section 13405(a);
- The right of individuals to receive electronic copies of their PHI maintained in an electronic health record, consistent with HITECH Section 13405(e); PTS shall support Client in providing such access to the extent technically feasible within the scope of Covered Services.

10C.8 PHI Handling Requirements

10C.8.1 Minimum Necessary

PTS shall access, use, and disclose PHI only to the minimum extent necessary to accomplish the intended purpose of the Covered Services, consistent with 45 C.F.R. § 164.514(d).

10C.8.2 De-identification

Where technically feasible and agreed upon in the applicable SOW, PTS shall use de-identified health information (consistent with the standards in 45 C.F.R. § 164.514(a)-(b)) in preference to PHI for purposes of testing, development, and analytics.

10C.8.3 Data Segregation

To the extent practicable, PTS shall maintain PHI in systems and repositories that are logically segregated from non-PHI Client Data and from data of other PTS clients.

10C.8.4 Retention

PHI shall be retained and disposed of in accordance with the BAA and applicable HIPAA Rules. Upon termination, PHI shall be returned or destroyed per Section 10C.10 of this Agreement.

10C.9 Co-Managed Risk Acceptance

Guardian Co-Managed clients applying this section must sign a risk acceptance acknowledging:

- The shared responsibility model means that Client's internal IT has direct access to and control over systems containing PHI;
- PTS's ability to maintain HIPAA-required safeguards depends on Client's internal IT personnel following PTS security procedures and configurations;
- PTS's liability for HIPAA-related incidents is reduced proportionally where the incident results from client-controlled actions or decisions, or from failure of Client's internal IT to follow PTS-prescribed security procedures.

10C.10 Termination

Upon termination of this section's applicability or the underlying SOW, PTS shall return or destroy PHI in its possession in accordance with the BAA and applicable HIPAA Rules. PTS shall certify in writing to Client the completion of such return or destruction within thirty (30) days of the termination date. If return or destruction is not feasible, PTS shall notify Client in writing, extend the protections of this section to the retained PHI, and limit further use or disclosure of such PHI.

10C.11 Limitations and Disclaimers

PTS is not a healthcare provider, health plan, healthcare clearinghouse, or covered entity under HIPAA. PTS's services under this section are limited to IT and security services as defined in the SOW. PTS does not provide clinical, billing, coding, legal, or operational healthcare services. PTS does not guarantee HIPAA compliance, audit outcomes, or Office for Civil Rights ("OCR") investigation results. Compliance with HIPAA Rules is ultimately Client's responsibility. Nothing in this section shall be construed as legal or compliance advice.

10C.12 Cross-References

Data protection obligations for non-PHI Client Data are governed by Section 10B of this Agreement (Data Protection Addendum). Incident response and breach notification procedures are governed by Section 9B of the MSA. Acceptable use obligations are governed by Section 5B of the MSA. Pricing for HIPAA-related services is governed by Section 12 of the MSA and the applicable SOW. Third-party and sub-processor obligations are governed by Section 11B of the MSA and Section 10B of this Agreement.

SECTION 11. TOOLS, MONITORING, AND AUTOMATION

11.1 Monitoring and Telemetry.

PTS deploys and operates monitoring agents, endpoint detection tools, and telemetry systems on Covered Assets as necessary to deliver Covered Services. Monitoring capabilities include, without limitation: real-time endpoint status monitoring, security event detection and alerting, patch compliance monitoring, backup status verification, system performance monitoring, and Microsoft 365 security alert monitoring. Client consents to PTS monitoring all Covered Assets and receiving telemetry and event data from those assets as a condition of the services.

PTS monitors only Covered Assets identified in the applicable SOW. PTS does not monitor personal devices, applications, or data outside the scope of Covered Assets. For Guardian Residential clients, PTS monitors only household devices expressly listed in the SOW and does not monitor personal communications, browsing activity, or content except as necessary for security purposes.

11.2 Remote Access and Automation Consent.

By executing an SOW under this Agreement, Client grants PTS a limited, non-exclusive license to remotely access, manage, and automate processes on Covered Assets for the purpose of delivering Covered Services. Remote access is secured using PTS-approved tools and multi-factor authentication. PTS personnel access Client systems only as necessary to perform Covered Services and in accordance with PTS's access control policies. PTS maintains audit logs of remote access sessions to Covered Assets.

Client may revoke remote access consent by providing written notice to PTS. Revocation of remote access consent will result in PTS's inability to deliver Covered Services, and PTS shall have no liability for any service failures, security incidents, or other consequences arising from such revocation. Revocation of remote access consent shall constitute grounds for PTS to terminate the affected SOW under Section 13.8.

11.3 Automation.

PTS may use automated scripts, workflows, and processes to deliver Covered Services. Automation is used to improve efficiency, consistency, and response time. PTS maintains documentation of automated processes and shall notify Client of significant changes to automated processes that materially affect the scope or nature of Covered Services.

SECTION 11B. THIRD-PARTY SERVICES

11B.1 PTS Standard Stack.

PTS delivers Covered Services using a curated set of approved third-party tools, platforms, and technologies (the "PTS Standard Stack"). The PTS Standard Stack is selected, vetted, and standardized by PTS to ensure consistency, security, and quality across the client base. Client must accept the PTS Standard Stack as a condition of enrollment in any managed Guardian Tier (Residential, Fundamentals, Compliance, Co-Managed).

11B.2 Standard Stack Components.

The PTS Standard Stack includes, but is not limited to, the following categories of tools (specific tools within each category are selected by PTS and may change from time to time with reasonable notice):

- Remote Monitoring and Management (RMM): tools for remote monitoring, management, patch deployment, and automation;
- Endpoint Detection and Response (EDR): tools for real-time threat detection, behavioral analysis, and response;

- Managed Detection and Response (MDR) / Security Operations Center (SOC): 24/7 security monitoring, alert triage, and response;
- Email Security: spam filtering, anti-phishing, and email threat protection;
- Web Filtering (DNS): DNS-layer web content filtering and threat blocking;
- Cloud Backup and Recovery: image-based cloud backup and disaster recovery for endpoints and servers;
- Microsoft 365 Management: partner-managed Microsoft 365 tenant administration and security;
- Password Management: enterprise password manager for credential management;
- Security Awareness Training: training platform for end-user cybersecurity education;
- Dark Web Monitoring: credential monitoring on the dark web;
- Documentation and Asset Management: IT documentation and asset inventory platform.

11B.3 Stack Modifications.

PTS may modify the PTS Standard Stack at any time to improve security, functionality, or cost-efficiency. For material stack changes (changes that affect the primary tool delivering a major service category), PTS shall provide at least thirty (30) days' written notice and shall work with Client to minimize disruption. Migration costs associated with PTS-initiated stack changes shall be borne by PTS unless the change is required by a vendor's unilateral action outside PTS's control.

11B.4 Non-Standard Tools.

Client-requested tools outside the PTS Standard Stack may be accommodated at PTS's discretion, subject to: (a) PTS's assessment that the non-standard tool does not create security, operational, or support conflicts; (b) additional fees for integration, support, and management of non-standard tools; and (c) the Client's agreement that PTS's liability caps are reduced proportionally for incidents attributable to non-standard tools. PTS is not obligated to support or integrate non-standard tools.

11B.5 Third-Party Vendor Relationships.

PTS maintains contractual relationships with vendors whose tools comprise the PTS Standard Stack. PTS negotiates, manages, and is responsible for these vendor relationships in connection with delivering Covered Services. Client acknowledges that: (a) third-party tools are subject to the terms and conditions of their respective vendors; (b) PTS is not responsible for vendor outages, price changes, feature changes, or discontinuations; (c) vendor changes that materially affect Covered Services will be communicated to Client with reasonable notice; and (d) PTS passes through any required vendor compliance obligations to Client through this Agreement and applicable SOWs.

11B.6 Client-Procured Third-Party Services.

Where Client procures third-party services independently (e.g., internet service providers, cloud platforms, software licenses, hardware vendors), Client is solely responsible for managing those relationships. PTS may coordinate with Client's third-party vendors as a convenience but does not assume responsibility for their performance, availability, or compliance. PTS's obligation extends only to integration with Client-procured services within the scope of Covered Services as specified in the applicable SOW.

SECTION 11C. AI SERVICES

APPLICABILITY: This Section 11C applies only to clients whose applicable SOW expressly includes AI Services. This section does not apply to clients whose SOW does not include AI Services.

This Section 11C governs PTS's use of artificial intelligence ("AI") tools, platforms, and services in connection with Covered Services.

11C.1 Purpose and Scope

This section governs the use of artificial intelligence ("AI") tools, platforms, and services by PTS in connection with Covered Services. AI Services may include machine learning models, natural language processing tools, automated threat detection, predictive analytics, and other AI-powered capabilities. This section applies only to clients whose applicable SOW expressly includes AI Services.

11C.2 Availability by Tier

AI Services under this section are available based on the client's enrolled Guardian Tier as follows:

Guardian Tier	AI Services Availability	Billing
Guardian Ad-Hoc	Not available	AI Services require minimum Compliance or Co-Managed tier
Guardian Residential	Not available	AI Services are not offered at the Residential tier
Guardian Fundamentals	Not available	AI Services are not offered at the Fundamentals tier unless separately agreed in writing
Guardian Compliance	Available — AI-powered security analytics, threat detection, and compliance automation as specified in SOW	Included in Compliance tier recurring fees per applicable SOW
Guardian Co-Managed	Available — AI-powered security monitoring, threat detection, and operational automation as specified in SOW	Included in Co-Managed tier recurring fees per applicable SOW

AI Services are not available at the Ad-Hoc, Residential, or Fundamentals tiers unless separately agreed in writing by an authorized representative of PTS. Any such separate written agreement constitutes an amendment to the applicable SOW.

11C.3 AI Service Descriptions

Specific AI Services to be provided are defined in the applicable SOW. The following table describes the AI Services that may be available under this section:

AI Service	Description
Automated Threat Detection and Alerting	AI-powered analysis of security telemetry to detect anomalous behavior, malware indicators, and intrusion attempts; generates prioritized alerts for PTS analyst review
AI-Assisted Vulnerability Prioritization	Machine learning models assess and rank vulnerabilities based on exploitability, asset criticality, and threat intelligence context
Behavioral Analytics (UEBA)	User and entity behavior analytics to detect insider threats, compromised credentials, and anomalous access patterns
Automated Compliance Evidence Collection	AI-assisted tools to gather, organize, and map compliance control evidence for frameworks such as NIST CSF, CIS Controls, and SOC 2
AI-Powered Helpdesk Triage and Routing	Automated classification and routing of support tickets based on natural language processing and historical resolution data

AI Service	Description
Predictive Analytics	Capacity planning and risk forecasting using historical data, asset telemetry, and threat intelligence feeds

11C.4 Data Use and Privacy

Client Data processed by AI tools is governed by Section 10 of the MSA and Section 10B of this Agreement (Data Protection Addendum). The following specific data use restrictions apply to AI Services:

- PTS shall not use Client Data to train general-purpose AI models without Client's express prior written consent;
- Client Data processed by AI tools shall be used only for the purpose of delivering the specific AI Service to Client as specified in the SOW;
- Anonymized and aggregated data — where it is not possible to re-identify any individual or Client — may be used to improve PTS's AI tools, service quality, and model performance;
- PTS shall disclose to Client any third-party AI platforms or vendors processing Client Data as part of AI Services, consistent with the sub-processor disclosure requirements in Section 10B of this Agreement;
- Client consents to PTS's use of approved AI platforms and vendors to process Client Data as necessary to deliver AI Services, subject to the data protection safeguards in Section 10B of this Agreement.

11C.5 AI-Generated Output Disclaimer

AI tools are supplementary to, not substitutes for, human judgment and expertise. The following disclaimers apply to all AI-generated outputs delivered by PTS:

- PTS does not guarantee the accuracy, completeness, or reliability of AI-generated outputs, recommendations, alerts, or analyses;
- AI tools may produce false positives (incorrectly flagging benign activity as a threat), false negatives (failing to detect an actual threat), or erroneous recommendations;
- All critical AI-generated outputs are subject to human review by PTS personnel before any action is taken on Client's behalf;
- AI-generated compliance evidence, reports, or assessments are provided as informational tools only and do not constitute legal, regulatory, or professional opinions;
- PTS assumes no liability for Client decisions made in reliance on AI-generated outputs without independent verification.

PTS DISCLAIMS ALL WARRANTIES WITH RESPECT TO AI SERVICES, INCLUDING WITHOUT LIMITATION WARRANTIES OF ACCURACY, COMPLETENESS, AND FITNESS FOR A PARTICULAR PURPOSE. AI SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE."

11C.6 AI Tool Usage Policies

The following policies govern PTS's use of AI tools in connection with Covered Services:

- PTS shall use AI tools only for purposes consistent with this section and the applicable SOW;
- PTS shall not use AI tools in a manner that violates applicable law, discriminates against individuals on the basis of protected characteristics, or compromises Client Data security;
- PTS shall maintain documentation of AI tools and platforms used to deliver AI Services and shall provide a summary to Client upon request;
- PTS reserves the right to modify, replace, or discontinue specific AI tools or platforms, provided that the AI Services described in the SOW continue to be delivered at the same or higher quality level;

- PTS shall notify Client of any material change to the AI tools or platforms used to deliver AI Services within thirty (30) days of such change.

11C.7 Client Consent and Acknowledgment

By executing an SOW that incorporates this section, Client:

- Consents to PTS's use of AI tools, platforms, and services as described in this section and the applicable SOW;
- Acknowledges the limitations of AI technology, including the potential for inaccuracies, false positives, false negatives, and evolving capabilities;
- Agrees that PTS's AI-generated outputs do not replace Client's independent judgment and that Client remains responsible for its own business and compliance decisions;
- Agrees to notify PTS of any concerns regarding AI usage, including any perceived ethical concerns, compliance conflicts, or data handling issues;
- Acknowledges that PTS's AI Services are subject to the same acceptable use policies as other Covered Services under Section 5B of the MSA.

11C.8 Ethical Use

PTS commits to the responsible and ethical use of AI in service delivery. PTS shall not use AI tools in a manner that violates applicable law, discriminates against individuals, or compromises Client Data security. PTS applies human oversight to all critical AI outputs. Client shall promptly notify PTS of any concerns regarding AI usage, and PTS shall investigate and respond in good faith within a reasonable timeframe.

11C.9 Liability

PTS's liability for AI Services is subject to the limitation of liability provisions in Section 16 of the MSA. PTS shall not be liable for:

- Decisions made by Client based on AI-generated outputs, where Client has not sought independent verification of material conclusions;
- The inherent limitations and unpredictability of AI technology;
- Errors or inaccuracies in AI-generated outputs arising from incomplete, inaccurate, or unrepresentative input data provided by or on behalf of Client;
- Changes in AI tool performance resulting from updates to third-party AI platforms or underlying models.

11C.10 Cross-References

Data protection obligations for AI Services are governed by Section 10B of this Agreement (Data Protection Addendum). Acceptable use obligations are governed by Section 5B of the MSA. Pricing for AI Services is governed by Section 12 of the MSA and the applicable SOW. Third-party AI platform terms are governed by Section 11B of the MSA.

SECTION 12. FEES AND PAYMENT

12.1 Fees and Billing.

All fees for Covered Services are set forth in the applicable SOW or Order Form. Fees are billed monthly in advance for recurring managed services, unless otherwise specified in the SOW. PTS invoices Client on the first day of each billing cycle. All invoices are due and payable within fifteen (15) calendar days of the invoice date.

12.2 Late Payment.

Invoices not paid within fifteen (15) calendar days of the invoice date will accrue interest at the rate of one and one-half percent (1.5%) per month (or the maximum rate permitted by applicable law, whichever is less), calculated from the invoice due date until the date of payment. PTS reserves all rights provided under applicable law for collection of unpaid amounts, including the right to initiate collection proceedings and to recover reasonable attorneys' fees and costs.

12.3 Disputed Invoices.

If Client disputes any portion of an invoice in good faith, Client must: (a) pay all undisputed amounts by the invoice due date; (b) provide PTS with written notice of the disputed amount within fifteen (15) days of the invoice date, specifying the basis for the dispute in reasonable detail. The parties shall use commercially reasonable efforts to resolve the dispute within thirty (30) days of receipt of the dispute notice. Interest does not accrue on disputed amounts during good-faith dispute resolution; however, if it is determined that Client's dispute was not made in good faith, interest accrues from the original invoice due date.

12.4 Payment Method.

PTS accepts the following payment methods: ACH/electronic funds transfer; check; credit card (subject to a processing fee as specified in the SOW); and any other method agreed between the parties in writing. Client shall provide valid payment information to PTS and keep it current. PTS may change accepted payment methods upon reasonable notice.

12.5 Onboarding Fees.

One-time onboarding fees, if applicable, are specified in the SOW. Onboarding fees are due upon execution of the SOW and are non-refundable unless PTS fails to commence onboarding within sixty (60) days of the agreed start date through no fault of Client.

12.6 Project and Out-of-Scope Fees.

Out-of-Scope Services and project-based work are billed at the rates specified in the SOW or, if not specified, at PTS's then-current standard rates. PTS will provide a written estimate for significant out-of-scope work before commencing. Emergency out-of-scope work may be commenced without prior estimate in time-critical situations, with PTS providing an estimate as soon as practicable.

12.7 Taxes.

Fees set forth in this Agreement are exclusive of all applicable sales, use, excise, value-added, goods and services, and similar taxes and government charges ("Taxes"). Client is responsible for paying all Taxes imposed on the services, unless Client provides PTS with a valid tax exemption certificate. PTS will collect and remit applicable Taxes as required by law. If PTS is required to pay any Taxes that are Client's responsibility, Client shall reimburse PTS promptly upon invoice.

12.8 Fee Adjustments for Scope Changes.

Monthly recurring fees will be adjusted to reflect: (a) increases in the number of covered devices, users, locations, or services ordered by Client; (b) decreases in scope, subject to any minimum commitment specified

in the SOW; and (c) any changes to the PTS Standard Stack that materially affect the cost of services. Fee adjustments take effect at the beginning of the next billing cycle following the scope change, unless the change is effective mid-cycle, in which case fees are prorated.

12.9 Suspension for Nonpayment.

If Client fails to pay any undisputed invoice within thirty (30) calendar days of the due date, PTS may suspend all or part of the Covered Services upon ten (10) days' written notice to Client. PTS will restore services within a commercially reasonable timeframe after all overdue amounts (plus any applicable late fees and Restoration Fees) have been paid in full. During the suspension period, Client remains obligated to pay all recurring fees and charges.

12.10 Prepayment Options.

Clients who elect to prepay for an annual term (twelve months or more) may be eligible for a prepayment discount as specified in the applicable SOW. Prepaid fees are non-refundable except as expressly stated in the applicable SOW. Prepayment discounts do not apply to one-time fees, project fees, or out-of-scope work.

12.11 Annual Price Adjustment.

PTS may adjust recurring fees annually upon sixty (60) days' written notice to Client. Annual price adjustments shall not exceed the greater of: (a) five percent (5%) of the then-current monthly recurring fees; or (b) the percentage change in the Consumer Price Index for All Urban Consumers (CPI-U), All Items, published by the U.S. Bureau of Labor Statistics for the twelve-month period ending three (3) months prior to the adjustment date. Fee adjustments take effect at the beginning of the billing cycle following the end of the notice period.

SECTION 13. TERM, SUSPENSION, TERMINATION, AND DISENGAGEMENT RIGHTS

13.1 Initial Term.

Unless otherwise specified in the applicable SOW, the initial term of this Agreement shall be twelve (12) months from the Effective Date (the "Initial Term"). If a SOW specifies a different initial term, the term specified in the SOW shall apply to that SOW. The Initial Term for each SOW runs independently; termination of one SOW does not automatically terminate other SOWs or this Agreement.

13.2 Renewal Term.

Upon expiration of the Initial Term, this Agreement (and each active SOW, unless otherwise specified in the SOW) shall automatically renew for successive periods equal in length to the Initial Term (each a "Renewal Term") unless either party provides written notice of non-renewal at least sixty (60) days prior to the expiration of the then-current term. Non-renewal notices must be delivered in accordance with Section 18.2 (Notices). Failure to provide timely non-renewal notice results in automatic renewal for the full Renewal Term.

13.3 Right to Suspend Services.

PTS may suspend all or part of the Covered Services, effective immediately or upon written notice as specified below, upon the occurrence of any of the following:

- Client's failure to pay undisputed fees when due (subject to the notice period in Section 12.9);
- Client's material breach of the Acceptable Use Policy (Section 5B);
- Client's failure to maintain Baseline Requirements (Section 5C of this Agreement) after written notice and a reasonable cure period of not less than fifteen (15) days;
- A Security Event requiring immediate isolation, containment, or quarantine of Client's environment to protect Client, PTS, or other PTS clients;
- Client's failure to cooperate with PTS in connection with a security investigation or incident response;
- Client's use of services for illegal purposes or in a manner that threatens the security, integrity, or availability of PTS's systems, tools, infrastructure, or other clients' environments;
- A court order, regulatory directive, subpoena, or law enforcement request requiring or recommending suspension;
- Client's insolvency, bankruptcy filing, or appointment of a receiver for a substantial portion of Client's assets.

13.4 Scope and Effect of Suspension.

During any period of suspension: (a) PTS shall maintain Client Data in accordance with its data protection obligations under this Agreement but shall have no obligation to deliver Covered Services; (b) Client remains obligated to pay all recurring fees and charges during the suspension period; (c) SLA response targets and other service level obligations are tolled; (d) PTS shall not be liable for any loss, damage, security exposure, or business disruption arising from suspension.

13.5 Restoration of Services.

PTS shall restore suspended services within a commercially reasonable timeframe after the condition giving rise to suspension has been fully remedied, verified by PTS, and PTS has confirmed in writing that restoration may proceed. PTS may charge a reasonable Restoration Fee to cover the costs of re-onboarding, re-assessment, re-configuration, or security verification necessitated by the suspension.

13.6 Termination for Cause.

Either party may terminate this Agreement or any SOW for cause upon written notice if the other party commits a material breach of this Agreement and fails to cure such breach within thirty (30) days after receiving written notice specifying the breach in reasonable detail (the "Cure Period"). If the breach is not reasonably susceptible to cure within thirty (30) days, the breaching party shall not be in default if it commences cure within the Cure Period and diligently pursues cure to completion. Notwithstanding the foregoing, PTS may terminate this Agreement immediately upon written notice, without a cure period, if Client: (a) engages in fraud, material misrepresentation, or illegal activity in connection with the services or this Agreement; (b) knowingly uses the services to cause harm to third parties; (c) repeatedly and materially violates the Acceptable Use Policy (Section 5B) after two or more prior written warnings; or (d) becomes insolvent, files for bankruptcy protection, or has a receiver appointed for a substantial portion of its assets.

13.7 Termination for Convenience.

Either party may terminate this Agreement or any SOW for convenience by providing at least ninety (90) days' written notice to the other party. If Client terminates for convenience prior to the expiration of the then-current term, Client shall pay an Early Termination Fee equal to the lesser of: (a) the total recurring fees remaining in the then-current term; or (b) three (3) months of recurring fees at the then-current monthly rate. The Early Termination Fee is due within thirty (30) days of the effective date of termination. The Early Termination Fee does not apply if Client terminates for PTS's uncured material breach under Section 13.6.

NOTE: Guardian Residential clients are subject to a different termination and early termination fee provision. Section 4B.9 of this Agreement supersedes and overrides this Section 13.7 for all Guardian Residential clients. Residential clients may terminate with thirty (30) days' written notice and the Early Termination Fee is capped at one (1) month of recurring fees.

13.8 PTS Disengagement Rights.

In addition to PTS's other termination rights, PTS may disengage from an active engagement, with thirty (30) days' written notice, if: (a) Client's environment poses an unreasonable security risk to PTS, PTS's other clients, or third parties that Client is unwilling to remediate within a reasonable timeframe; (b) Client's internal IT team, contractors, or authorized users repeatedly interfere with, circumvent, or undermine PTS's ability to deliver services; (c) the relationship between the parties has deteriorated to a degree that materially impairs PTS's ability to deliver services professionally; or (d) Client engages a direct competitor of PTS to provide services that overlap substantially with Covered Services and Client's continued engagement raises conflicts of interest that PTS cannot reasonably manage. Upon disengagement under this Section, PTS shall waive the Early Termination Fee and shall cooperate with Client in an orderly transition.

13.9 Survival.

The following provisions of this Agreement shall survive termination or expiration: Section 3 (Definitions); Section 10 (Data Protection and Confidentiality); Section 12 (Fees and Payment, with respect to amounts accrued through termination); Section 14 (Intellectual Property); Section 15 (Warranties and Disclaimers); Section 16 (Limitation of Liability); Section 17 (Indemnification); Section 18 (General Provisions); Section 19 (Governing Law and Dispute Resolution); and any provisions that by their nature should survive termination.

SECTION 14. INTELLECTUAL PROPERTY

14.1 Provider IP.

PTS retains all right, title, and interest in and to Provider IP, including without limitation all tools, scripts, software, code, methodologies, processes, templates, frameworks, documentation, training materials, playbooks, and know-how owned or developed by PTS before, during, or after the term of this Agreement. Nothing in this Agreement transfers, assigns, or conveys any ownership of Provider IP to Client.

14.2 Client IP.

Client retains all right, title, and interest in and to Client IP, including without limitation all Client Data, content, materials, trade secrets, trademarks, and proprietary business processes owned by Client. Nothing in this Agreement transfers, assigns, or conveys any ownership of Client IP to PTS.

14.3 Limited License Grants.

Client grants PTS a limited, non-exclusive, non-transferable, revocable license to access, use, copy, and process Client Data and Client IP solely as necessary to perform Covered Services during the term of this Agreement. PTS grants Client a limited, non-exclusive, non-transferable, revocable license to use PTS-provided tools, dashboards, portals, and software solely for Client's internal use in connection with Covered Services during the term of this Agreement. All licenses granted under this Section terminate automatically upon expiration or termination of this Agreement or the applicable SOW.

14.4 Feedback.

If Client provides PTS with any suggestions, ideas, enhancement requests, feedback, or recommendations regarding PTS's services, tools, or products ("Feedback"), PTS may use such Feedback without restriction, compensation, or attribution. Client hereby assigns to PTS all right, title, and interest in any Feedback.

14.5 Aggregated and Anonymized Data.

PTS may aggregate and anonymize data collected in the course of providing Covered Services for purposes of benchmarking, industry analysis, threat intelligence, product development, and service improvement. Aggregated and anonymized data shall not identify Client, any individual, or any specific Client system.

14.6 Open-Source Software.

PTS may use open-source software components in the delivery of Covered Services. PTS shall comply with applicable open-source license terms. Client acknowledges that open-source software is provided "as is" without warranty.

SECTION 15. WARRANTIES AND DISCLAIMERS

15.1 Limited Warranty.

PTS warrants that: (a) it will perform Covered Services in a professional and workmanlike manner, consistent with commercially reasonable industry standards and practices applicable to similar service providers in the managed IT and cybersecurity industry; (b) its personnel assigned to perform Covered Services have the qualifications, training, and experience reasonably necessary to perform such services; and (c) it has the legal right and authority to enter into this Agreement and perform its obligations hereunder.

15.2 DISCLAIMER OF WARRANTIES.

EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 15.1, PTS PROVIDES ALL SERVICES, TOOLS, SOFTWARE, DELIVERABLES, REPORTS, AND RECOMMENDATIONS ON AN "AS IS" AND "AS AVAILABLE" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PTS EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING WITHOUT LIMITATION ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, PTS MAKES NO WARRANTY OR REPRESENTATION AND DOES NOT GUARANTEE THAT: (A) SERVICES WILL PREVENT ALL SECURITY BREACHES, CYBERATTACKS, MALWARE INFECTIONS, RANSOMWARE ATTACKS, DATA LOSS, DATA THEFT, OR UNAUTHORIZED ACCESS; (B) SYSTEMS WILL OPERATE WITHOUT INTERRUPTION, ERROR, OR DOWNTIME; (C) ALL VULNERABILITIES, THREATS, OR SECURITY WEAKNESSES WILL BE IDENTIFIED, PRIORITIZED, OR REMEDIATED; (D) CLIENT WILL ACHIEVE OR MAINTAIN COMPLIANCE WITH ANY REGULATORY FRAMEWORK, INDUSTRY STANDARD, CERTIFICATION, OR CONTRACTUAL OBLIGATION; (E) DATA CAN BE RECOVERED IN ALL CIRCUMSTANCES, INCLUDING AFTER RANSOMWARE, HARDWARE FAILURE, OR DATA CORRUPTION; OR (F) PTS'S RECOMMENDATIONS, IF IMPLEMENTED, WILL PREVENT ANY SPECIFIC HARM OR LOSS.

15.3 Residential Additional Disclaimer.

For Guardian Residential clients, in plain language: PTS provides household IT and cybersecurity support services to help protect your home technology. However, PTS cannot guarantee that your home will be completely secure from all cyber threats. PTS is not responsible for security problems caused by household members' actions (such as clicking on phishing emails, sharing passwords, or installing risky software), unauthorized device modifications, or the use of devices or services that PTS does not manage.

SECTION 16. LIMITATION OF LIABILITY

16.1 EXCLUSION OF INDIRECT DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE SERVICES PROVIDED HEREUNDER, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, WARRANTY, OR OTHERWISE), INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF BUSINESS OPPORTUNITY, LOSS OF DATA, LOSS OF GOODWILL OR REPUTATION, BUSINESS INTERRUPTION, COST OF PROCUREMENT OF SUBSTITUTE SERVICES, OR ANY OTHER INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF THE DAMAGES WERE FORESEEABLE.

16.2 Tier-Specific Liability Caps.

Subject to the carve-outs in Section 16.4, the total aggregate liability of PTS to Client for all claims arising out of or related to this Agreement shall not exceed the applicable cap based on Client's Guardian Tier, as set forth in the following table:

Guardian Tier	Maximum Aggregate Liability Cap	Conditions / Notes
Guardian Ad-Hoc	Lesser of: (a) total fees paid for the specific service giving rise to the claim, OR (b) Five Thousand Dollars ($5,000)	Cap applies per service engagement. No ongoing managed service relationship. Client retains full responsibility for environment.
Guardian Residential	Lesser of: (a) two (2) months of recurring fees, OR (b) Ten Thousand Dollars ($10,000)	Client must maintain covered devices in compliance with Section 5C.2.3 of this Agreement (Residential Baseline). Consumer law protections under Section 4B of this Agreement apply.
Guardian Fundamentals	Lesser of: (a) three (3) months of recurring fees at the then-current monthly rate, OR (b) Twenty-Five Thousand Dollars ($25,000)	Client must be in compliance with Section 5C of this Agreement (Security Baseline Requirements) at the time of the incident giving rise to the claim. Non-compliance with Baseline Requirements at time of incident may reduce or void the cap in PTS's favor.
Guardian Compliance	Lesser of: (a) six (6) months of recurring fees at the then-current monthly rate, OR (b) Seventy-Five Thousand Dollars ($75,000)	Client must have participated in all required quarterly executive reviews and be in compliance with Section 5C of this Agreement at the time of the incident. Cap reflects elevated service scope and shared governance obligations.
Guardian Co-Managed	Lesser of: (a) six (6) months of recurring fees at the then-current monthly rate, OR (b) Seventy-Five Thousand Dollars ($75,000)	Cap is subject to proportional reduction for incidents resulting from client-controlled decisions, unauthorized changes by internal IT staff, or client delays in implementing PTS recommendations. The proportional reduction is determined by the degree to which client actions or omissions contributed to the incident, as documented in PTS's incident records.

16.2.1 Universal Liability Exclusions

Regardless of Guardian Tier, PTS shall not be liable under any circumstances for: (a) ransom or extortion payments; (b) business interruption losses; (c) lost profits, revenue, or business opportunities; (d) regulatory fines, penalties, or sanctions; (e) reputational harm or damage to goodwill; (f) data reconstruction or recovery

costs beyond PTS-managed backup scope; (g) damages from Client's failure to obtain cyber insurance; or (h) damages from Client's failure to implement PTS recommendations.

16.2.2 Carve-Outs

The caps set forth in Section 16.2 do not apply to: (a) Client's obligation to pay all fees and amounts due under this Agreement; (b) Client's indemnification obligations under Section 17 of this Agreement; (c) damages arising from a party's violations of the Acceptable Use Policy (Section 5B of this Agreement) causing direct harm to the other party; or (d) damages caused by a party's willful misconduct or gross negligence.

16.3 UNIVERSAL LIABILITY EXCLUSIONS.

IN ADDITION TO THE EXCLUSION OF INDIRECT DAMAGES IN SECTION 16.1, PTS SHALL NOT BE LIABLE UNDER ANY CIRCUMSTANCES FOR ANY OF THE FOLLOWING, REGARDLESS OF THE FORM OF ACTION, THEORY OF LIABILITY, OR WHETHER THE DAMAGE WAS FORESEEABLE: (A) RANSOM PAYMENTS OR EXTORTION PAYMENTS, WHETHER PAID BY CLIENT, CLIENT'S INSURER, OR ANY THIRD PARTY; (B) BUSINESS INTERRUPTION LOSSES, INCLUDING LOST PRODUCTION, DELAYED OPERATIONS, OR INABILITY TO CONDUCT BUSINESS; (C) LOST PROFITS, LOST REVENUE, OR LOST BUSINESS OPPORTUNITIES; (D) REGULATORY FINES, PENALTIES, SANCTIONS, OR ASSESSMENTS IMPOSED ON CLIENT BY ANY GOVERNMENTAL OR REGULATORY AUTHORITY; (E) REPUTATIONAL HARM, DAMAGE TO GOODWILL, OR LOSS OF CUSTOMER RELATIONSHIPS; (F) DATA RECONSTRUCTION, RE-ENTRY, RE-CREATION, OR RECOVERY COSTS BEYOND THE SCOPE OF PTS-MANAGED BACKUP AND RECOVERY SERVICES; (G) DAMAGES ARISING FROM CLIENT'S FAILURE TO OBTAIN OR MAINTAIN ADEQUATE CYBER LIABILITY INSURANCE; OR (H) DAMAGES ARISING FROM CLIENT'S FAILURE TO IMPLEMENT PTS'S RECOMMENDATIONS WITHIN AGREED TIMELINES.

16.4 Carve-Outs.

The liability caps set forth in Section 16.2, and the exclusions in Sections 16.1 and 16.3, shall not apply to: (a) Client's obligations to pay all fees, charges, and amounts due under this Agreement; (b) Client's indemnification obligations under Section 17; (c) damages arising from a party's violations of the Acceptable Use Policy (Section 5B) that cause direct harm to the other party; or (d) damages caused by a party's willful misconduct or gross negligence.

16.5 Essential Basis.

Client acknowledges that the limitations of liability set forth in this Section 16 reflect a reasonable allocation of risk between the parties and that PTS's pricing is based on this allocation of risk. These limitations shall apply regardless of whether any limited remedy fails of its essential purpose.

SECTION 17. INDEMNIFICATION

17.1 Mutual Indemnification.

Each party (the "Indemnifying Party") shall indemnify, defend, and hold harmless the other party and its officers, directors, members, managers, employees, agents, successors, and permitted assigns (collectively, the "Indemnified Parties") from and against all third-party claims, actions, suits, proceedings, investigations, demands, losses, damages, liabilities, judgments, settlements, costs, and expenses (including reasonable attorneys' fees and court costs) (collectively, "Losses") arising out of or resulting from the Indemnifying Party's: (a) material breach of this Agreement; (b) negligence or willful misconduct in connection with this Agreement; or (c) violation of applicable law in connection with this Agreement.

17.2 Client-Specific Indemnification.

In addition to its obligations under Section 17.1, Client shall indemnify, defend, and hold harmless PTS and the PTS Indemnified Parties from and against all Losses arising out of or resulting from:

- Client's or Client's authorized users' misuse of services or violation of the Acceptable Use Policy (Section 5B);
- Client's violation of applicable laws, regulations, or contractual obligations, including without limitation data protection laws, privacy laws, healthcare regulations, and financial services regulations;
- Acts, omissions, negligence, or failures of Client's third-party vendors, service providers, contractors, or internal staff;
- Security incidents caused by or attributable to Client's failure to maintain Baseline Requirements, implement PTS recommendations, or fulfill Client Responsibilities;
- Client's misrepresentation of material facts regarding Client's environment, compliance obligations, business activities, or eligibility for the selected Guardian Tier.

17.3 Indemnification Procedures.

The Indemnified Party seeking indemnification shall: (a) promptly notify the Indemnifying Party in writing of any claim or threatened claim for which indemnification is sought (provided that failure to provide prompt notice shall not relieve the Indemnifying Party of its obligations except to the extent it is materially prejudiced by the delay); (b) grant the Indemnifying Party sole control of the defense, investigation, and settlement of such claim; and (c) provide reasonable cooperation and assistance at the Indemnifying Party's expense. The Indemnifying Party shall not settle any claim that imposes any obligation, restriction, or liability on the Indemnified Party without the Indemnified Party's prior written consent, which shall not be unreasonably withheld.

SECTION 18. GENERAL PROVISIONS

18.1 Force Majeure.

Neither party shall be liable for any failure or delay in performing its obligations under this Agreement to the extent that such failure or delay is caused by a Force Majeure Event. For purposes of this Agreement, "Force Majeure Event" means an event or circumstance beyond the reasonable control of the affected party that could not have been reasonably foreseen or avoided, including without limitation: (a) natural disasters; (b) acts of government, regulatory authorities, or quasi-governmental entities; (c) war, armed conflict, terrorism, civil unrest, insurrection, or sabotage; (d) labor disputes, strikes, or work stoppages; (e) cyberattacks by third parties that are not specifically directed at the affected party's client (including distributed denial-of-service attacks, nation-state attacks, and widespread malware campaigns); (f) internet service provider, cloud service provider, or data center outages; (g) utility failures, including power outages and telecommunications failures; (h) supply chain disruptions; (i) pandemic, epidemic, or public health emergencies; and (j) government orders, mandates, quarantine requirements, or travel restrictions. The affected party shall: (i) provide prompt written notice to the other party; (ii) use commercially reasonable efforts to mitigate the effects of the Force Majeure Event; and (iii) resume performance as soon as reasonably practicable. If a Force Majeure Event continues for more than sixty (60) consecutive days, either party may terminate this Agreement upon written notice.

18.2 Notices.

All notices, requests, demands, consents, and other communications required or permitted under this Agreement shall be in writing and shall be delivered by: (a) personal delivery; (b) nationally recognized overnight courier (e.g., FedEx, UPS); (c) United States mail, postage prepaid, certified or registered, return receipt requested; or (d) email with confirmation of receipt. Notices to Client shall be sent to the address specified in the applicable SOW. Notices to PTS shall be sent to Phantom Technology Solutions, LLC, Attn: Legal Notices, 5097 N 600 E, Rolling Prairie, Indiana 46371, with a copy by email to legal@phantomts.com. Either party may update its notice address by written notice to the other party. Notices are effective upon receipt by the intended recipient.

18.3 Amendment.

This Agreement may be amended, modified, or supplemented only by a written instrument that expressly references this Agreement, identifies the specific provisions being amended, and is executed by authorized representatives of both parties. No oral agreement, course of dealing, course of performance, or trade usage shall modify the terms of this Agreement. PTS reserves the right to update this Agreement from time to time by posting a revised version at https://www.phantomts.com/legal/msa. PTS will provide at least thirty (30) days' written notice to active clients of any material changes. Continued use of services after the notice period constitutes acceptance of the updated terms. For changes that materially reduce Client's rights or materially increase Client's obligations, Client may terminate the affected SOW within the thirty-day notice period without payment of an Early Termination Fee.

18.4 Waiver.

No waiver of any breach or default of this Agreement shall constitute a waiver of any prior, concurrent, or subsequent breach or default. No waiver shall be effective unless made in writing and signed by an authorized representative of the waiving party.

18.5 Severability.

If any provision of this Agreement is held to be invalid, illegal, or unenforceable by a court of competent jurisdiction, such provision shall be modified to the minimum extent necessary to make it valid, legal, and enforceable while preserving the parties' original intent. If such modification is not possible, the provision shall be severed from this Agreement, and the remaining provisions shall continue in full force and effect.

18.6 Entire Agreement and Integration.

This Agreement, together with all SOWs and Order Forms executed hereunder, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, representations, understandings, negotiations, and discussions, whether oral or written. This Agreement specifically supersedes and excludes: (a) AI-generated proposals, estimates, scoping documents, or outputs; (b) chatbot outputs, automated responses, or auto-generated communications; (c) marketing materials, brochures, presentations, website content, case studies, or promotional communications; and (d) informal communications including emails, text messages, instant messages, or verbal discussions not reduced to a written amendment executed in accordance with Section 18.3.

18.7 Counterparts and Electronic Signatures.

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Delivery of an executed counterpart by email (including PDF), facsimile, or electronic signature platform shall be as effective as delivery of an original executed counterpart. Electronic signatures, including signatures executed via DocuSign, Adobe Sign, or similar electronic signature platforms, are valid, binding, and enforceable and shall have the same legal force and effect as original ink signatures, in accordance with the Indiana Uniform Electronic Transactions Act (Ind. Code § 26-2-8 et seq.) and the federal Electronic Signatures in Global and National Commerce Act (E-SIGN Act, 15 U.S.C. § 7001 et seq.).

18.8 Assignment.

PTS may assign this Agreement, in whole or in part, without Client's prior consent in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of PTS's assets or equity interests. PTS may also assign this Agreement to an affiliate or successor entity without Client's consent. Client may not assign this Agreement, in whole or in part, without PTS's prior written consent, which shall not be unreasonably withheld, conditioned, or delayed. Any attempted assignment in violation of this Section shall be null and void.

18.9 No Third-Party Beneficiaries.

This Agreement is for the sole and exclusive benefit of the parties hereto and their permitted successors and assigns. Nothing in this Agreement, express or implied, is intended to confer upon any third party any rights, remedies, obligations, or benefits under or by reason of this Agreement.

18.10 Independent Contractor.

The relationship between PTS and Client is that of independent contractor. PTS personnel are not employees, agents, partners, or joint venturers of Client. Nothing in this Agreement creates or is intended to create a partnership, joint venture, franchise, agency, or employment relationship between the parties.

18.11 Non-Solicitation.

During the term of this Agreement and for a period of twelve (12) months following termination or expiration for any reason, Client shall not, directly or indirectly, solicit, recruit, hire, engage, or attempt to solicit, recruit, hire, or engage (whether as an employee, independent contractor, consultant, advisor, or in any other capacity) any employee, contractor, or subcontractor of PTS who was involved in delivering Covered Services to Client at any time during the twelve (12) months preceding the solicitation or attempted solicitation, without PTS's prior written consent. If Client hires or engages any such individual in violation of this provision, Client shall pay PTS a placement fee equal to fifty percent (50%) of the individual's first-year total compensation (including base salary, bonuses, and benefits) as liquidated damages, which the parties agree is a reasonable estimate of PTS's damages and not a penalty.

18.12 Reference Authorization.

Client consents to PTS identifying Client as a customer of PTS and using Client's name and logo in PTS's marketing materials, website, case studies, client listings, proposals, and promotional communications, subject to the following conditions: (a) PTS shall not disclose Client's Confidential Information in any marketing materials without Client's prior written consent; (b) PTS shall not misrepresent the nature or scope of services provided; and (c) Client may revoke this consent at any time by written notice to PTS, and PTS shall cease using Client's name and logo within thirty (30) days of receiving such notice. This consent does not authorize PTS to disclose any financial, security, or operational details about Client's engagement without separate written consent.

18.13 Publicity.

Except as permitted by Section 18.12, neither party shall issue press releases, public announcements, or other publicity regarding this Agreement, the services, or the business relationship without the prior written consent of the other party. Either party may disclose the existence of this Agreement (but not the terms or pricing of any SOW or Order Form) if required by applicable law, regulation, or court order.

18.14 Anti-Corruption.

Each party represents, warrants, and covenants that in connection with this Agreement it will comply with all applicable anti-bribery and anti-corruption laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and any applicable local equivalents. Neither party shall offer, pay, promise, or authorize any payment or transfer of anything of value, directly or indirectly, to any government official, government employee, or any other person for the purpose of improperly influencing any official act or decision.

18.15 Export Controls.

Each party shall comply with all applicable export control laws and regulations, including the U.S. Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). Client shall not export, re-export, or transfer any PTS services, software, or technical data in violation of applicable export control laws. Client represents that it is not on any U.S. government restricted party list.

SECTION 19. GOVERNING LAW AND DISPUTE RESOLUTION

19.1 Governing Law.

This Agreement shall be governed by and construed in accordance with the laws of the State of Indiana, without regard to its conflict of laws rules or principles that would result in the application of the laws of another jurisdiction.

19.2 Informal Negotiation.

Before initiating any formal dispute resolution proceeding (including mediation or litigation), the parties shall attempt in good faith to resolve any dispute, claim, or controversy arising out of or relating to this Agreement through informal negotiation. The aggrieved party shall deliver written notice to the other party describing the dispute, the specific provisions at issue, and the relief sought (the "Dispute Notice"). The parties shall have thirty (30) days from the date of the Dispute Notice to resolve the dispute through direct negotiation between authorized representatives with decision-making authority. During the negotiation period, neither party shall commence formal proceedings (except for emergency injunctive relief to prevent irreparable harm).

19.3 Mediation.

If the parties are unable to resolve a dispute through informal negotiation within the thirty-day period specified in Section 19.2, the parties shall submit the dispute to mediation before commencing litigation. Mediation shall be administered by the American Arbitration Association (AAA) or JAMS, at the election of the party initiating the mediation. The mediation shall be conducted in Indiana or by video conference if in-person mediation is impracticable. Each party shall bear its own costs and attorneys' fees in connection with mediation; the costs of the mediator shall be shared equally. If the parties cannot resolve the dispute through mediation within sixty (60) days of the mediation demand, either party may pursue litigation in accordance with Section 19.4.

19.4 Litigation; Venue and Jurisdiction.

If the parties are unable to resolve a dispute through informal negotiation and mediation, either party may initiate litigation. The parties irrevocably consent to the exclusive jurisdiction and venue of the state and federal courts located in La Porte County, Indiana for all disputes arising out of or relating to this Agreement. Each party waives any objection to the jurisdiction or venue of such courts and waives any defense of inconvenient forum. The prevailing party in any litigation shall be entitled to recover its reasonable attorneys' fees, court costs, and other legal expenses from the non-prevailing party.

19.5 Residential Client Dispute Resolution.

Notwithstanding Sections 19.2 through 19.4, Guardian Residential clients may elect to resolve disputes through the Indiana Consumer Protection Division or through small claims court if the amount in dispute does not exceed the jurisdictional limit of Indiana small claims courts. Nothing in this Agreement limits any right Residential clients may have under applicable consumer protection laws.

19.6 Limitation on Claims.

Any claim or cause of action arising out of or related to this Agreement must be brought within two (2) years of the date on which the aggrieved party knew or should have known of the basis for the claim. Any claim or cause of action not brought within this period is permanently barred, regardless of any applicable statute of limitations.

SECTION 20. EXECUTION AND ACCEPTANCE

This Agreement does not require separate execution by Client. Client's execution of any Statement of Work that references or incorporates this Master Services Agreement constitutes full and binding acceptance of all terms contained herein, as of the date such Statement of Work is executed.

PTS executes this Agreement by posting it at https://www.phantomts.com/legal/msa and by executing Statements of Work with individual clients. The version of this Agreement in effect at the time of SOW execution governs that engagement, subject to the amendment provisions of Section 18.3.

For questions about this Agreement, contact Phantom Technology Solutions, LLC at: 5097 N 600 E, Rolling Prairie, Indiana 46371 | (800) 338-4474 | support@phantomts.com | www.phantomts.com