

MASTER SERVICES AGREEMENT

Version 1.4 | Effective September 3, 2026

Rollout AI, Inc.

These terms govern any services expressly described in a signed Order Form, Statement of Work, or Addendum. No service is included or excluded by this Agreement unless the applicable signed service document says so.

How This Agreement Works

These Master Services Terms ("Terms" or "Agreement") set out the rights and obligations of Rollout AI, Inc. ("Company") and each client ("Client") for services that the parties agree to in a signed Service Document.

Service Documents. A "Service Document" means an Order Form, Statement of Work, or Addendum signed by both parties. It identifies the SKU or individual services purchased and states the applicable quantities or baseline counts, fees, payment terms, effective date, coverage hours, add-ons, and customer-specific overrides. A proposal, service description, or catalog is part of a Service Document only if the signed Service Document incorporates it by reference.

Selected Services. "Selected Services" means every service and component identified in the SKU, plan, line item, or service description incorporated into a signed Service Document, together with any separately listed add-on. Selecting a SKU is sufficient to select all components included in that SKU; the parties do not need to list each component again in the Service Document.

Embedded Service Schedules. Schedules A through D are part of this Agreement and state reusable terms for the services they describe. When a Selected Service corresponds to a service component described in a Schedule, that Schedule applies automatically. A Schedule states how an ordered service is delivered; it does not independently add a service to the engagement or assign a service to a particular SKU. Section A.6 states the default Initial Response Time objectives for relevant Managed IT support services unless the applicable Service Document expressly provides different objectives.

Order of Precedence. If documents conflict, they control in the following order for the matter addressed: (1) the most recently signed Addendum or Statement of Work; (2) the signed Order Form; and (3) these Master Services Terms.

Standard Terms. These Terms are the Company's standard published terms. Customer-specific scope and commercial terms, including any approved override, must appear in a Service Document signed by both parties.

Plan and Tool Changes. The Company may change plan names or composition for future orders and Renewal Terms. A change to a future plan or catalog does not reduce Selected Services during the current Term unless the parties agree in writing. The Company may substitute a reasonably comparable third-party tool used to deliver the same Selected Service as permitted by Section 13.

Agreement Terms

This section, together with the service schedules below and each applicable Service Document, constitutes the agreement between the Company and Client.

1. Services

During the applicable Term, the Company will provide the Selected Services. A signed Service Document may select a SKU, plan, individual service, or add-on. If it selects a SKU or plan, every service component included in the incorporated SKU or plan description is a Selected Service even if the Service Document does not repeat each component.

Schedules A through D apply automatically to the corresponding Selected Services and provide the standard delivery terms, dependencies, responsibilities, and exclusions for those services. A service description in this Agreement does not independently add the service to Client's scope or assign it to a particular SKU.

A service, deliverable, or obligation outside the Selected Services is outside the agreed scope. The Company is not required to provide changed or additional work unless authorized in a signed amendment, new Service Document, or other written change authorization that states the applicable fees and timing.

2. Duties of the Parties

A. Company. The Company will use commercially reasonable efforts to deliver the Services in accordance with the applicable Service Document, these Terms, and applicable industry standards. The Company will assign qualified personnel and maintain documentation reasonably appropriate for the Services. The Company will maintain its own business continuity and disaster recovery plan.

B. Client. Client will: (i) maintain a valid payment method as required by Section 3 and the Service Document; (ii) provide reasonable access to facilities, systems, information, and personnel needed for the Services; (iii) designate an authorized point of contact; (iv) complete the responsibilities allocated to Client; and (v) give timely notice of changes that may affect the Services. Client consents to remote access reasonably required to perform the Services.

C. Service Levels. For Managed IT support services to which response-time objectives are relevant, the Initial Response Time objectives in Section A.6 apply unless the applicable Service Document expressly states different objectives. Those objectives apply only during Standard Business Hours. A ticket submitted outside Standard Business Hours is deemed received at the beginning of the next Standard Business Hours period for purposes of measuring Initial Response Time. No response-time objective applies outside Standard Business Hours unless the applicable Service Document expressly states the after-hours coverage and objective. Availability, coverage, recovery, resolution, or other service-level commitments apply only if expressly stated in the Service Document. All response and resolution measures are objectives and depend on Client cooperation and third-party availability.

3. Pricing and Payment

A. Fees. Fees and rates are stated in the applicable Service Document. No fee or rate stated in a proposal, website, price list, or prior discussion applies unless incorporated into a signed Service Document.

B. Payment Method and ACH Authorization. Recurring fees will be paid by ACH debit unless the applicable Service Document expressly permits another payment method. Client authorizes the Company to initiate ACH debits from the designated account for amounts due on or after each invoice date and will provide a completed authorization and valid banking information before the Effective Date. Client may revoke authorization with thirty (30) days' prior written notice only if it establishes another payment method accepted by the Company.

before the next invoice date. The Company is not responsible for Client bank fees. Any discount or exception associated with a payment method applies only if expressly stated in the Service Document.

C. Payment Terms. Recurring Services fees are invoiced in advance and collected on or after the invoice date. Hardware, software, licensing, and third-party services procured for Client are due upon receipt unless the Service Document states otherwise.

D. Late Payment. An undisputed amount not received within twenty (20) days after the invoice date bears interest at eighteen percent (18%) per annum (1.5% per month), or the maximum lawful rate, whichever is less. The Company may suspend affected Services after five (5) business days' written notice and may charge a reinstatement fee equal to five (5) days of the then-current recurring Services fee before resuming. Client will pay reasonable collection costs, court costs, and attorneys' fees incurred to collect delinquent amounts.

E. Fee Disputes. Client must give written notice of an invoice dispute within thirty (30) days after the invoice date and identify the disputed amount and basis. Undisputed amounts remain due. A dispute not raised within thirty (30) days is waived.

F. Annual List-Price Increases. Recurring fees will not increase during an annual Term except as expressly stated in the applicable Service Document. Effective at the start of a Renewal Term, the Company may increase an applicable list price upon at least thirty (30) days' prior written notice. As of any renewal date, the cumulative increase in the list price for a service or item may not exceed six percent (6%) compounded for each completed twelve-month period since that service or item was first priced in a Service Document. The Company may apply all or part of unused cumulative increase capacity in a later Renewal Term. The starting list price is the undiscounted list price stated when the service or item is first ordered; if no undiscounted list price is stated, it is the recurring rate stated at that time. Expiration or reduction of an introductory, promotional, or first-year discount expressly identified in the Service Document is not a list-price increase and does not count toward this cap. Changes resulting from scope, quantity, usage, taxes, third-party pass-through charges, or additional services also do not count toward the cap.

G. Taxes. Fees exclude applicable taxes. Client will pay them unless it provides a valid exemption certificate.

H. Quantity and Usage Adjustments. If pricing depends on users, devices, locations, storage, transactions, or another variable measure, the measurement method, baseline or minimum, and adjustment timing are those stated in the Service Document. An adjustment within the agreed pricing method does not require an amendment; a change outside it does.

4. Term and Termination

A. Initial Term. The Agreement for each Service Document begins on its effective date and continues for the initial term stated there. If the Service Document is silent, the Initial Term is one (1) year.

B. Renewal. Upon expiration of the Initial Term, the Agreement automatically renews for successive one (1)-year periods ("Renewal Terms") unless either party provides at least ninety (90) days' prior written notice of non-renewal before the end of the then-current Term.

C. Termination for Cause. Either party may terminate an affected Service Document upon written notice if: (i) the other party materially breaches and fails to cure within twenty (20) days after notice, or ten (10) days for non-payment; (ii) the other party files or has filed against it a bankruptcy or insolvency petition not dismissed within sixty (60) days; or (iii) Client or Client personnel engage in abusive or threatening conduct toward Company personnel, in which case the Company may terminate on ten (10) days' notice.

D. Remedies for Early Termination. If the Company terminates for cause, or if Client purports to terminate, cancels, or ceases receiving the Services without cause before the expiration of the then-current Term, Client will pay a termination fee equal to all recurring fees due through the remainder of the then-current Term at the fees in effect as of the termination date. Nothing in this Section grants either party a right to terminate for convenience. If Client terminates for cause, Client is responsible only for fees for Services properly delivered through the effective termination date.

E. Transition and Offboarding. Upon expiration or termination, each party will return the other's equipment, software, and materials and cooperate in good faith with transition. Requested transition assistance is billed at the applicable rate. The Company will retain Client Data for thirty (30) days unless the Service Document or law requires another period. Client is responsible for transferring data and establishing replacement services before termination.

F. Transition from Prior Provider. If an ordered Service includes transition from another provider, the Company will use commercially reasonable efforts to coordinate with that provider. The Company is not responsible for the prior provider's acts or omissions or for pre-existing conditions not caused by the Company. Any shared-responsibility period will be governed by the allocation in the Service Document or transition plan.

5. Ownership

Materials, intellectual property, software tools, scripts, documentation, and work product developed by the Company before or independently of an engagement ("Company Property") remain Company property. Client receives no license except as expressly stated in these Terms or a Service Document. Client's pre-existing materials, data, and intellectual property ("Client Property") remain Client property. Client grants the Company a limited right to use Client Property only as necessary to provide the Services. Non-third-party software installed or provided by the Company remains Company property unless a Service Document says otherwise.

6. Confidential Information

A. Definition. "Confidential Information" means non-public information disclosed by one party ("Disclosing Party") to the other ("Receiving Party") in connection with the Agreement that is designated confidential or reasonably should be understood as confidential, including trade secrets, technical data, business plans, financial information, customer lists, pricing, software and source code, security practices, network configurations, personnel information, and the terms of the Agreement.

B. Exclusions. Confidential Information does not include information that: (i) becomes public without breach by the Receiving Party; (ii) was rightfully known without restriction before disclosure; (iii) is rightfully received from a third party without restriction; or (iv) is independently developed without use of the Disclosing Party's Confidential Information.

C. Obligations. Each party will protect the other's Confidential Information using at least reasonable care, use it only to perform or receive the Services, and disclose it only to personnel, contractors, and advisors who need to know and are bound by obligations no less protective than these Terms.

D. Compelled Disclosure. A Receiving Party may disclose Confidential Information if required by law or court order, provided it gives prompt notice when legally permitted, cooperates in seeking protection, and limits disclosure to what is required.

E. Survival. Confidentiality obligations survive termination in perpetuity for trade secrets and for three (3) years for other Confidential Information.

7. Non-Solicitation of Employees

During the Term and for twelve (12) months after expiration or termination, Client will not directly or indirectly solicit for employment, hire, or engage a person who was employed or contracted by the Company during the preceding twelve (12) months and was involved in Client's Services. For a breach, Client will pay liquidated damages, not a penalty, equal to twenty-four (24) months of that person's compensation at the rate paid by the Company during the last full month of the engagement. The Company may also seek injunctive relief without proving actual damages or posting a bond.

8. Force Majeure

Neither party is liable for delay or failure caused by circumstances beyond its reasonable control, including natural disasters, pandemic, fire, flood, war, terrorism, civil unrest, labor disputes, government action, or power, telecommunications, or internet-provider failure. The affected party will promptly notify the other and use commercially reasonable efforts to reduce impact. Force majeure does not excuse payment of amounts already due.

9. Representations and Warranties

Each party represents and warrants that: (i) it has the full right, power, and authority to enter into and perform this Agreement; (ii) the execution and performance of this Agreement have been duly authorized by all necessary action; (iii) this Agreement constitutes a valid and binding obligation, enforceable in accordance with its terms; and (iv) the execution and performance of this Agreement do not and will not violate any agreement, order, or law to which such party is a party or by which it is bound.

10. Disclaimer of Warranties

EXCEPT AS EXPRESSLY STATED IN THE AGREEMENT, THE COMPANY MAKES NO EXPRESS OR IMPLIED WARRANTY, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, FOR SERVICES, HARDWARE, SOFTWARE, OR THIRD-PARTY SERVICES. THE COMPANY DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE SERVICES, FREEDOM FROM UNAUTHORIZED ACCESS, OR DETECTION OR PREVENTION OF EVERY SECURITY THREAT OR VULNERABILITY. SERVICES ARE PROVIDED "AS IS."

11. Cybersecurity

A. General Acknowledgment. Cybersecurity threats evolve continuously, no transmission or system is completely secure, and service effectiveness depends on Client's own administrative, technical, and physical safeguards and cooperation.

B. Company Disclaimer. The Company does not guarantee Client security or a specific security level, is not liable for acts or errors of Client personnel or providers, and is not required to implement a Client safeguard unless it is included in a Service Document.

C. Client Cyber Insurance. Client represents that it maintains cyber liability insurance of at least One Million Dollars (\$1,000,000) per occurrence and in the annual aggregate, covering liability arising from theft, dissemination, or use of electronic confidential or personal data and from malicious code or damage to third-party systems or data. Client will provide evidence upon request, unless the Service Document expressly states another requirement.

12. Devices Outside Agreed Scope

If the Services include device or network management, the Company is not required to support a device that is outside the scope defined in the Service Document. Client assumes the risk of connecting an unmanaged or

unknown device to the covered environment. The Company is not responsible for an issue caused by such a device.

13. Third-Party Management Tools and Vendors

The Company may use third-party vendors and software to provide Services. Those relationships may change. The Company may replace a third-party product or tool with a reasonably comparable alternative used to deliver the same Selected Service and will use commercially reasonable efforts to notify Client if the change materially affects Client's environment or use of the Services. A substitution does not by itself change the Selected Services or fees. Any material scope or fee change requires the process stated in the applicable Service Document or Section 3. Client remains responsible for third-party relationships not assigned to the Company.

14. Limitation of Liability

THE LIABILITY LIMITS IN THIS SECTION ARE A MATERIAL PART OF THE PARTIES' PRICING AND RISK ALLOCATION. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE COMPANY WILL NOT BE LIABLE TO CLIENT OR A THIRD PARTY FOR INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATED TO THE AGREEMENT OR SERVICES, INCLUDING LOST PROFITS, LOST DATA, LOST GOODWILL, BUSINESS INTERRUPTION, OR EQUIPMENT DOWNTIME, REGARDLESS OF THEORY OF LIABILITY AND EVEN IF ADVISED OF THE POSSIBILITY.

THE COMPANY'S AGGREGATE LIABILITY TO CLIENT FOR ALL CLAIMS ARISING OUT OF OR RELATED TO THE AGREEMENT OR THE SERVICES WILL NOT EXCEED THE TOTAL FEES PAID BY CLIENT TO THE COMPANY DURING THE SIX (6)-MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST OCCURRENCE GIVING RISE TO LIABILITY. CLIENT ACKNOWLEDGES THAT THIS LIMIT WAS A MATERIAL INDUCEMENT FOR THE COMPANY TO ENTER INTO THE AGREEMENT AT THE AGREED FEES.

15. Indemnification

Client will indemnify, defend, and hold harmless the Company and its principals, officers, directors, employees, and agents from claims, liabilities, damages, losses, costs, and expenses, including reasonable attorneys' fees, arising from: (i) Client's breach of the Agreement; (ii) Client's negligence or willful misconduct; (iii) Client's violation of law; or (iv) a third-party claim arising from Client's data, systems, or business operations.

16. General Terms

A. Entire Agreement. These Terms and the applicable Service Documents are the entire agreement on their subject matter and supersede prior discussions and agreements. A modification is valid only in a writing signed by authorized representatives, except for a written change authorization permitted by the applicable Service Document.

B. Severability. If a provision is unenforceable, it will be modified only as needed to be enforceable and the remainder will continue.

C. Waiver. A failure or delay in exercising a right is not a waiver. A waiver must be in writing.

D. Assignment. Neither party may assign the Agreement without prior written consent, except the Company may assign it in a merger, acquisition, or sale of substantially all assets on thirty (30) days' notice.

E. Independent Contractors. The parties are independent contractors. The Agreement does not create a partnership, joint venture, employment, agency, or franchise relationship.

F. No Third-Party Beneficiaries. The Agreement benefits only the parties and their permitted successors and assigns.

G. Electronic Execution. Service Documents may be executed in counterparts and by electronic signature, each of which is valid and binding.

H. Survival. Sections 5, 6, 7, 14, 15, and 18, and Client's obligation to pay amounts due, survive expiration or termination.

I. Marketing and Publicity. Client grants the Company a non-exclusive, royalty-free, worldwide license to use Client's name, logo, and a general description of Services in marketing, case studies, proposals, and public communications. The Company will not disclose details of Client's environment or operations without prior written consent. Client may revoke the license on written notice, effective within thirty (30) days.

J. Feedback. Feedback about Services or Company products is non-confidential and Company property. Client assigns all rights in Feedback to the Company, which may use it without obligation, compensation, or attribution.

17. Notices

A notice under the Agreement must be in writing and sent by email to the address in the applicable Service Document or a later address provided in writing. Email notice is delivered when sent to the correct address. Each party will keep its address current. For default, termination, or material breach, the sender is encouraged to also use overnight courier or certified mail.

18. Dispute Resolution

A. Management Resolution. Before formal proceedings, authorized representatives will discuss a dispute in good faith for thirty (30) days after written notice.

B. Arbitration. An unresolved dispute will be finally resolved by binding arbitration administered by the American Arbitration Association under its Commercial Arbitration Rules before one arbitrator experienced in information technology services contracts. Arbitration will take place in Wilmington, Delaware unless the parties agree otherwise. The arbitrator will issue a reasoned written decision, and judgment may be entered by a court with jurisdiction.

C. Governing Law; Venue. Delaware law governs without regard to conflicts principles. The parties consent to exclusive jurisdiction in state and federal courts in New Castle County, Delaware for compelling arbitration, enforcing an award, or seeking emergency equitable relief.

D. Prevailing Party Fees. The prevailing party in arbitration or an action to enforce an award may recover reasonable attorneys' fees and costs.

E. Injunctive Relief. Either party may seek emergency equitable relief to prevent irreparable harm, including a breach of confidentiality or intellectual property rights, without posting a bond.

Schedule A: Managed IT Services Terms

A.1 Applicability and Scope

This Schedule applies whenever the Selected Services include Managed IT Services or a managed service component described below. The Service Document selects the SKU or services, covered users, devices and locations, quantities, support coverage, and fees. This Schedule supplies the standard delivery terms for each selected component without assigning any component to a particular SKU.

A.2 Service Components and Delivery Terms

Each service description in this Section applies only when the corresponding service component is included in the Selected Services. The descriptions below state the terms for those components and do not add them to Client's scope.

Remote support. The Company will provide remote troubleshooting and assistance for covered users, devices, applications, and systems through the designated support channels. Support is remote-first. Messages sent directly to Company personnel are not treated as support tickets and do not start a response-time measurement unless the Company confirms ticket creation.

On-site support. The Company will provide on-site support for covered systems as stated in the Service Document. Other on-site work may be provided as Additional Services or when reasonably required to complete covered remote support and approved by Client. Applicable coverage windows, travel charges, and rates are stated in the Service Document or approved change authorization.

Monitoring and alerting. Company tools may collect device, system, network, and security telemetry and generate automated alerts at all hours when the applicable platform supports it. Automated monitoring is not continuous human observation and does not create an after-hours response obligation. Alerts are reviewed and acted on during the applicable coverage hours unless the Service Document expressly includes after-hours coverage.

Patch management. The Company will use commercially reasonable efforts to deploy approved operating-system and supported third-party application updates to covered devices during maintenance windows. Patch availability, compatibility, device connectivity, vendor behavior, and required restarts may affect timing. Patch management does not guarantee that every vulnerability will be patched or that an update will not cause disruption.

Endpoint and device management. The Company may install remote monitoring and management, mobile device management, endpoint detection and response, or similar agents on covered devices. Client will not disable, remove, or materially reconfigure those agents without the Company's written approval. These controls reduce risk but do not guarantee detection, prevention, or remediation of every event or threat.

Identity and cloud administration. The Company will administer covered identity, email, productivity, or cloud platforms, including user provisioning, deprovisioning, access changes, and configuration support within the agreed administrative scope. The Service Document identifies covered platforms and whether Company or Client procures related licenses.

Onboarding and offboarding. The Company will perform the technical onboarding, role-change, and offboarding tasks included in the applicable service description. Client remains responsible for employment decisions, access approvals, asset recovery, and timely notice under Section A.3.

Administrative access. The Company may use its own systems, platforms, credentials, agents, and tools to provide the ordered services. Client receives administrative access to Company-managed tools only if the

applicable Service Document expressly grants it. Client will provide the Company with physical and remote access to Client systems reasonably necessary for the ordered services.

Co-management. If the parties agree to co-manage any system or function, the Service Document will identify the parties' respective responsibilities and access rights. The Company is not responsible for an action taken by Client, Client personnel, or another provider outside that allocation.

Cloud productivity backup. The Company will configure and administer backup for the covered accounts and workloads in the identified cloud productivity platform. Retention, storage, restore scope, and account coverage are governed by the Service Document or the selected service's documented configuration. Backup may not capture data that a platform, license, account state, or vendor interface makes unavailable. The Company does not guarantee that every item can be restored.

Server backup and disaster recovery. The Company will provide the backup, replication, testing, or recovery services stated for the covered systems. Any recovery point objective, recovery time objective, retention period, test-restoration commitment, or guaranteed capacity applies only if expressly stated in the Service Document.

Email security and encryption. The Company will configure and administer the covered filtering, anti-phishing, anti-malware, impersonation-protection, or encryption controls. Such systems may produce false positives or false negatives. Client remains responsible for appropriate user judgment, escalation, and lawful email use.

DNS and web filtering. The Company will administer filtering policies for covered users, devices, or networks. Filtering may block legitimate content or permit unwanted content. Client will promptly report suspected misclassification and remains responsible for business decisions about allowed content.

Password management. The Company will provision or administer the identified password-management platform. Client is responsible for user adoption, accurate account recovery information, protection of master credentials, and compliance with the platform provider's terms.

Domain and DMARC protection. The Company will monitor or configure supported email-authentication controls for covered domains. These controls reduce spoofing risk but cannot prevent every misuse of a domain, look-alike domain, display name, or third-party sending service.

Security awareness and phishing simulation. The Company will provide the training, testing, campaigns, or reporting stated in the service description. Client will ensure required participation and determine any personnel response. Training and simulation do not guarantee that users will identify or avoid every threat.

Firewall and network management. The Company will administer covered network devices, configurations, and locations. Internet service providers, utilities, public networks, building systems, and equipment not identified as covered remain outside Company control.

Reviews, reporting, and roadmaps. The Company will provide reviews, reports, inventories, recommendations, or technology roadmaps at the frequency and for the audience stated in the selected service description or Service Document.

A.3 Client Responsibilities

To the extent reasonably applicable to the ordered Managed IT Services, Client will:

- designate a primary contact authorized to approve changes, access requests, and invoices;
- maintain supported, properly licensed hardware, operating systems, and software that meet any minimum standards stated in the Service Document;
- maintain manufacturer or vendor support for systems that require it under the Service Document;
- provide at least seven (7) business days' notice for planned new users, twenty-four (24) hours' notice of a termination when practicable, and forty-eight (48) hours' notice of a role or access change, unless the Service Document states another period;

- provide at least fourteen (14) days' notice of a planned material environment change and notice of an emergency change as soon as practicable;
- submit support requests through the designated channels communicated by the Company and provide enough information for reasonable triage;
- not disable Company-installed tools, agents, security controls, or administrative access without prior written approval;
- ensure required users participate in any ordered or required security training;
- maintain the cyber liability insurance required by Section 11; and
- cooperate with reasonable security, access, maintenance, and remediation requirements necessary to provide the ordered services.

Delay, added cost, or risk caused by Client's failure to meet these responsibilities may require a written change, may be billed as Additional Services if authorized, and may excuse the Company's affected performance to the extent caused by that failure.

A.4 Standard Exclusions

Unless included in the Selected Services, the following are outside scope: major projects or changes; new locations, relocations, mergers, or significant expansions; hardware repair, replacement, or purchase costs; custom software or web development; forensic investigation, incident response, e-discovery, legal hold, or data recovery beyond a selected service; legal, regulatory, or insurance advice; support for uncovered, unlicensed, or unsupported devices and applications; remediation of pre-existing conditions; work caused by an unauthorized change; disputes with a third-party vendor; and failures of internet, utility, carrier, or other services outside Company control. The Company may quote or perform excluded work as Additional Services only with written authorization.

A.5 Changes and Additional Services

A request that changes the signed scope, assumptions, quantities, responsibilities, schedule, or deliverables requires written approval by authorized representatives. The parties will document any additional fees, timing, and terms in an amended Service Document or other written change authorization before the Company is required to perform the changed work.

A.6 Service Level Objectives

This Section applies only when the Selected Services include Managed IT support services to which response-time objectives are relevant. Unless the applicable Service Document expressly states different objectives, the following Initial Response Time objectives apply only during Standard Business Hours.

"Initial Response Time" means the elapsed time from ticket creation to first acknowledgment and assignment by a Company technician. Response-time objectives apply to remote support. Resolution times are objectives and depend on issue complexity and Client cooperation. "Standard Business Hours" ("SBH") are the support hours stated in the applicable Service Document. A ticket submitted outside SBH is deemed received at the beginning of the next SBH period for purposes of measuring Initial Response Time. No response-time objective applies outside SBH unless the applicable Service Document expressly states the after-hours coverage and objective.

Issue Description	Priority	Initial Response Objective (SBH)
Service unavailable: all users and core functions down (for example, server or internet outage)	P1: Critical	30 min.

Issue Description	Priority	Initial Response Objective (SBH)
Significant service degradation: many users or critical functions affected	P2: High	2 hrs.
Limited degradation: few users affected; business can continue	P3: Medium	4 hrs.
Minor issue: single user affected; business process uninterrupted	P4: Low	8 hrs.

Schedule B: Web Development Services Terms

B.1 Applicability and Scope

This Schedule applies whenever the Selected Services include web design, development, maintenance, hosting administration, or related services. The Service Document selects the covered websites or applications, deliverables, capacity, milestones, fees, and any customer-specific terms. This Schedule supplies the standard terms for those Selected Services.

B.2 Client Materials and Cooperation

Client will timely provide content, brand assets, credentials, access, approvals, and other materials reasonably required for the ordered services. Client represents that it has the rights needed for the Company to use Client-provided materials for the engagement. A Client delay extends affected delivery dates and may require a written change to scope or fees.

B.3 Delivery and Acceptance

If the Service Document includes a deliverable but does not state an acceptance procedure, Client will have ten (10) business days after delivery to accept it or give written notice describing specific material defects. If Client does not give that notice within the review period, the deliverable is deemed accepted. The Company will use commercially reasonable efforts to correct a timely reported defect that makes the deliverable materially nonconforming with the signed scope.

B.4 Third-Party Services and Costs

Hosting, domains, plugins, software licenses, stock assets, payment processors, and other third-party products or services are included only if the Service Document says so. Third-party products and services remain subject to their providers' terms, availability, and changes.

B.5 Standard Exclusions

Unless included in the Selected Services, web services exclude a major redesign, a new website or application, custom functionality outside agreed capacity, content creation, accessibility or regulatory certification, search-ranking or traffic guarantees, incident response, and third-party fees. The Company does not guarantee browser, device, plugin, or platform compatibility beyond the supported environments stated in the Service Document or applicable service description.

Schedule C: Chief AI Officer Services Terms

C.1 Applicability and Scope

This Schedule applies whenever the Selected Services include Chief AI Officer ("CAIO") advisory services, AI tool development, workflows, automations, integrations, or related maintenance and support. The Service Document selects the applicable work, deliverables, capacity, milestones, fees, and customer-specific terms. Each service description below applies only to the corresponding CAIO service included in the Selected Services. Advisory services do not constitute legal, financial, or regulatory compliance advice.

C.2 Service Delivery

Advisory services. The Company will provide the strategy, assessment, planning, governance, training, or operating support stated in the applicable service description or Service Document. Client remains responsible for management decisions and implementation outside the selected scope.

AI tools and automations. The Company will design, configure, develop, or integrate the identified tools, workflows, or automations. Performance depends on Client systems, data quality, access, third-party platforms, and Client cooperation. Material changes to requirements, data sources, integrations, or usage may require written change authorization.

Maintenance and support. The Company will provide the maintenance, monitoring, changes, or support stated in the Service Document. Third-party model, API, or platform changes may require an adjustment to functionality, timing, or fees under an approved change.

C.3 Delivery and Acceptance

If the Service Document includes a deliverable but does not state an acceptance procedure, Client will have ten (10) business days after delivery to accept it or provide written notice describing specific material defects. If Client does not provide notice within that period, the deliverable is deemed accepted.

C.4 Intellectual Property

Company Ownership. Unless a Service Document expressly states otherwise, all AI tools, code, software, algorithms, models, model configurations, fine-tuned weights, prompts, system prompts, workflow designs, automation logic, integrations, and documentation created in connection with CAIO services ("Developed IP") are the exclusive property of the Company. To the extent any Developed IP qualifies as a work made for hire, it is so designated; to the extent it does not, Client hereby irrevocably assigns all right, title, and interest to the Company.

No Transfer. Nothing in this Agreement constitutes a sale, transfer, or assignment of Developed IP to Client except as expressly stated in a Service Document. Client's rights are limited to the license in Section C.5.

Pre-Existing IP. The Company retains all rights in tools, code, frameworks, models, and methodologies developed before or independently of this Agreement. Client retains ownership of its pre-existing data and systems and grants the Company a limited license to use them solely to provide the ordered services.

Non-Exclusive Development. The Company may develop similar tools for other clients. The Company will not disclose Client's Confidential Information, but may use general knowledge, techniques, and patterns refined through the engagement.

C.5 License Grant

Subscription License. Subject to timely payment and compliance with this Agreement, the Company grants Client a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to access and use the Developed IP identified in the Service Document solely for Client's internal business operations, in the delivered form, during the applicable Term.

Suspension for Non-Payment. If Client fails to pay an undisputed amount within ten (10) days after its due date, the Company may suspend access to affected AI tools until all overdue amounts are paid, subject to any notice requirement in Section 3.D.

License Restrictions. Client may not: (i) copy, distribute, sell, sublicense, rent, lease, or transfer Developed IP; (ii) reverse engineer, decompile, or attempt to derive source code, model weights, system prompts, or underlying algorithms; (iii) modify or create derivative works without prior written consent; (iv) use an AI tool to develop a competing product or service; or (v) represent that Client owns or developed the AI tools, except to the extent a Service Document expressly permits the action.

C.6 Acceptable Use

Client will use AI tools only for the internal business purposes stated in the Service Document and will not use them to violate law, third-party rights, or applicable platform terms; facilitate unauthorized access; engage in fraud, phishing, impersonation, harassment, or abuse; or generate unlawful or infringing content. Client will maintain appropriate human review for consequential decisions informed by AI outputs.

C.7 AI Output Disclaimer

AI outputs may be inaccurate, incomplete, biased, or inconsistent. The Company does not warrant that AI outputs will be accurate, complete, error-free, or fit for a particular purpose. Client is responsible for verification and for ensuring that its use complies with applicable law and regulation.

C.8 Data and Third-Party Platforms

Client Data. Client Data remains Client's property. The Company will use it only to provide the ordered CAIO services and will disclose it only as needed to operate those services or as required by law.

Third-Party Platforms. AI tools may use third-party platforms. Client's use is subject to those platforms' terms and data practices. The Company will use enterprise-tier API access where commercially available and will not use Client's Confidential Information to fine-tune models for other clients without written consent.

Data Return. Upon expiration or termination of the applicable CAIO services, the Company will return or make available Client Data within thirty (30) days and delete or destroy it from Company systems within sixty (60) days, except as required by law or stated in the Service Document.

Schedule D: Compliance and Security Assessment Services Terms

D.1 Applicability and Scope

This Schedule applies whenever the Selected Services include SOC 2 readiness or operations, policy or control support, evidence collection, trust-center or questionnaire support, GRC platform access, audit facilitation, penetration testing, or another compliance or security assessment service. The Service Document selects the applicable scope, systems and entities, deliverables, milestones, fees, and customer-specific terms. Each service description below applies only to the corresponding compliance or security assessment service included in the Selected Services. This Schedule does not require the purchase of any other service.

D.2 Service Delivery

Readiness and program support. The Company will perform the assessment, gap analysis, policy development, control design, implementation support, evidence collection, or recurring compliance operations stated in the applicable service description or Service Document.

Trust center and questionnaires. The Company will help administer the identified trust center, security questionnaires, or customer assurance materials. Client must review and approve representations about its organization, systems, controls, and compliance status before external use.

GRC platform. The Company will provision or administer the identified governance, risk, and compliance platform. Platform access, functionality, retention, exports, and third-party terms remain subject to the applicable license and Service Document.

Audit facilitation. The Company will coordinate within the agreed scope with an independent auditor. The auditor is not the Company's employee or agent, retains independent judgment, and may require additional evidence, testing, remediation, or fees.

Penetration testing and security assessments. Testing will be limited to the systems, dates, methods, and rules of engagement approved in writing by Client. The Company may use a qualified third-party tester. Testing is point-in-time and is not exhaustive; it may not identify every weakness. Retesting is included only if stated in the Selected Services.

D.3 Responsibility Allocation and System Access

The Service Document will identify which operational and engineering controls are assigned to the Company and which remain Client's responsibility. Any control, remediation task, system, or environment not assigned to the Company remains Client's responsibility. The Company will access a production environment, cloud console, source-code repository, or other restricted system only to the extent authorized in the Service Document or in a later written authorization by Client.

D.4 Client Responsibilities

Compliance Lead. Client will designate at least one employee or contractor authorized to make compliance decisions, provide evidence, respond to auditor inquiries, and coordinate with the Company.

Timely Participation. Client will respond to reasonable information and evidence requests, participate in scheduled sessions, review documentation, and complete responsibilities within the timelines stated in the Service Document or project plan.

Pre-Existing Issues. Before readiness work begins, Client will disclose known security incidents, data breaches, regulatory investigations, prior audit findings, and material control deficiencies relevant to the engagement.

Auditor Cooperation. Client will cooperate with the independent auditor and provide timely access to personnel, systems, and documentation as required for the audit, subject to the agreed responsibility and access allocation.

D.5 No Guarantee of Compliance or Assessment Outcome

The Company does not guarantee a SOC 2 Type I or Type II report, certification, clean opinion, successful assessment, absence of vulnerabilities, or any favorable finding. Outcomes depend on matters outside the Company's control, including Client's controls and participation, the accuracy of Client information, third-party performance, testing limitations, and an auditor's or assessor's independent judgment. An adverse or delayed outcome alone is not a breach by the Company.

D.6 Enhanced Confidentiality for Compliance Materials

Policies, procedures, risk assessments, audit evidence, GRC data, gap analyses, and audit reports generated for the engagement ("Compliance Materials") are Client Confidential Information. The Company will disclose Compliance Materials only to the auditor, a GRC provider as necessary, another recipient authorized by Client, or as required by law. Upon expiration or termination of the applicable compliance services, the Company will provide a complete export within thirty (30) days and then delete or destroy the materials from Company systems, except as required by law.

D.7 Compliance-Specific Limitation of Liability

In addition to Section 14, the Company is not liable for: (i) failure to achieve a certification or particular audit or assessment outcome; (ii) an auditor's or assessor's qualified opinion, exception, or adverse finding; (iii) loss, penalty, regulatory action, or reputational harm resulting from a failed, delayed, or adverse audit or assessment; (iv) a vulnerability not identified by point-in-time testing; (v) a control, system, or task not assigned to the Company; or (vi) an act or omission of the auditor, tester, GRC provider, or another third party not under the Company's control.

Version 1.4 | Effective September 3, 2026