

MASTER SERVICES AGREEMENT

Third-Party Vendor Risk Management Edition

Agreement Date: [DATE]

Client: [CLIENT LEGAL NAME] (“Client”)

Vendor: [VENDOR LEGAL NAME] (“Vendor”)

Agreement No.: [MSA-____-____]

CONFIDENTIAL — EXECUTION COPY

TABLE OF CONTENTS

Article 1 – Definitions	3
Article 2 – Services	5
Article 3 – Term and Termination	7
Article 4 – Fees, Invoicing, and Payment	9
Article 5 – Confidentiality	11
Article 6 – Data Protection and Privacy	13
Article 7 – Intellectual Property	17
Article 8 – Security	19
Article 9 – Audit Rights	20
Article 10 – Representations and Warranties	21
Article 11 – Indemnification	23
Article 12 – Limitation of Liability	25
Article 13 – Insurance	26
Article 14 – Subcontractors and Subprocessors	27
Article 15 – Business Continuity and Disaster Recovery	28
Article 16 – Incident Response and Notification	29
Article 17 – AI-Specific Provisions	31
Article 18 – Compliance with Laws	33
Article 19 – Force Majeure	34
Article 20 – Dispute Resolution	35
Article 21 – General Provisions	36
Exhibit A – Statement of Work	
Exhibit B – Service Level Agreement	
Exhibit C – Fee Schedule	
Exhibit D – IT Security Addendum	
Exhibit E – Data Processing Agreement	
Exhibit F – Approved Subprocessors	

MASTER SERVICES AGREEMENT

This Master Services Agreement (“Agreement”) is entered into as of [DATE] (“Effective Date”) by and between:

[CLIENT LEGAL NAME], a [state/jurisdiction] [corporation/LLC/other] with its principal place of business at [Address] (“Client”);

and

[VENDOR LEGAL NAME], a [state/jurisdiction] [corporation/LLC/other] with its principal place of business at [Address] (“Vendor”).

Client and Vendor are each referred to herein individually as a “Party” and collectively as the “Parties.”

RECITALS

WHEREAS, Client desires to engage Vendor to provide certain services as described herein and in the applicable Statements of Work;

WHEREAS, Vendor has the expertise, qualifications, and capacity to provide such services;

WHEREAS, the Parties desire to establish the terms and conditions governing their relationship;

NOW, THEREFORE, in consideration of the mutual covenants and agreements set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

ARTICLE 1 – DEFINITIONS

 **GUIDANCE:** This section establishes the entire defined-term glossary. Every capitalized term used in the Agreement should be defined here. Courts construe ambiguities against the drafter, so precision in definitions is critical. Add or remove defined terms as the deal requires.

As used in this Agreement, the following terms have the meanings set forth below:

"Affiliate" means, with respect to a Party, any entity that directly or indirectly controls, is controlled by, or is under common control with such Party, where "control" means ownership of more than fifty percent (50%) of the voting interests of the subject entity.

"AI System" means any machine-based system that, for a given set of objectives, makes predictions, recommendations, or decisions influencing real or virtual environments. AI Systems include, without limitation, machine learning models, large language models, generative AI tools, automated decision-making systems, and natural language processing systems.

"Authorized User" means Client's employees, contractors, and agents who are authorized by Client to access and use the Services under this Agreement.

"Background IP" means all Intellectual Property Rights owned or licensed by a Party prior to the Effective Date, or developed or acquired by a Party independently of the Services.

"Change Order" means a written instrument signed by authorized representatives of both Parties that modifies the scope, timeline, or fees set forth in a Statement of Work.

"Client Data" means all data, content, information, and materials submitted, uploaded, or otherwise provided by or on behalf of Client or its Authorized Users to Vendor in connection with the Services, including Personal Data.

"Confidential Information" has the meaning set forth in Article 5.

"Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Client Data transmitted, stored, or otherwise processed by or on behalf of Vendor, including any breach of security leading to any of the foregoing.

"Data Processing Agreement" means the data processing agreement attached hereto as Exhibit E, which governs Vendor's processing of Personal Data on behalf of Client.

"Deliverable" means any work product, report, software, documentation, or other tangible output that Vendor is required to deliver to Client pursuant to a Statement of Work.

"Effective Date" has the meaning set forth in the preamble.

"Force Majeure Event" has the meaning set forth in Article 19.

"Intellectual Property Rights" means all patents, copyrights, trademarks, trade secrets, moral rights, database rights, and all other intellectual property and proprietary rights recognized in any jurisdiction worldwide.

"IT Security Addendum" means the IT security requirements attached hereto as Exhibit D, as may be updated by Client from time to time upon reasonable notice.

"Key Personnel" means the Vendor employees or contractors identified in a Statement of Work as critical to delivery of the Services.

"Malicious Code" means viruses, worms, time bombs, Trojan horses, ransomware, spyware, adware, and other malicious or harmful code, files, scripts, agents, or programs.

"Personal Data" means any information relating to an identified or identifiable natural person, including without limitation information subject to any applicable Privacy Law.

"Privacy Laws" means all applicable laws and regulations relating to the processing of Personal Data, including without limitation the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), and all comparable state, national, and international privacy laws.

"Security Incident" has the meaning set forth in Article 16.

"Services" means the services described in the applicable Statement of Work, including any professional services, software-as-a-service, managed services, or other services provided by Vendor to Client.

"Service Level Agreement" or "SLA" means the service level commitments set forth in Exhibit B.

"Statement of Work" or "SOW" means a written document executed by both Parties that describes a specific set of Services, Deliverables, timelines, and fees under this Agreement.

"Subcontractor" means any third party engaged by Vendor to perform any portion of the Services. For purposes of data processing, Subcontractors who process Personal Data are referred to as "Subprocessors."

"Term" has the meaning set forth in Section 3.1.

"Work Product" means all Deliverables and any other work product, inventions, developments, improvements, discoveries, and intellectual property created by Vendor specifically for Client pursuant to this Agreement and paid for by Client.

ARTICLE 2 – SERVICES

GUIDANCE: The Services article defines what Vendor must do and how changes are managed. A well-drafted SOW reference clause prevents scope creep and establishes the governing hierarchy between the MSA and individual SOWs. Generally the MSA should govern in conflicts unless the SOW expressly overrides a specific provision.

2.1 Scope of Services

- 2.1.1** Vendor shall provide the Services described in each Statement of Work executed by the Parties. Each SOW is incorporated into and governed by this Agreement. In the event of a conflict between this Agreement and a SOW, this Agreement shall govern unless the SOW expressly states that it supersedes a specific provision of this Agreement.
- 2.1.2** Vendor shall perform the Services in a professional and workmanlike manner, using qualified personnel with the skills, knowledge, and experience necessary to deliver the Services in accordance with this Agreement and the applicable SOW.
- 2.1.3** Vendor shall comply with all applicable laws, regulations, and industry standards in the performance of the Services, including but not limited to those relating to data protection, privacy, cybersecurity, and export controls.

GUIDANCE: Section 2.1.3 is a broad compliance hook. Supplement with a specific Compliance with Laws article (Article 18) that identifies statutes by name relevant to your sector (HIPAA, GLBA, PCI-DSS, DORA, EU AI Act, etc.).

2.2 Statements of Work

- 2.2.1** Each SOW shall set forth, at minimum: (a) a detailed description of the Services; (b) the Deliverables and acceptance criteria therefor; (c) the timeline and key milestones; (d) the fees and payment schedule; (e) Key Personnel; (f) Client responsibilities and dependencies; and (g) any applicable service levels.
- 2.2.2** No SOW shall be binding unless signed by authorized representatives of both Parties. A purchase order issued by Client shall not constitute a SOW and shall not alter the terms of this Agreement.

2.3 Change Orders

- 2.3.1** Either Party may request changes to the scope of Services under an existing SOW by delivering a written change request to the other Party. Vendor shall provide a written impact assessment within ten (10) business days describing the effect of the proposed change on fees, timeline, and resource requirements.
- 2.3.2** No change to a SOW shall be effective unless set forth in a Change Order signed by authorized representatives of both Parties. Vendor shall not commence work on any change until a Change Order is fully executed.

GUIDANCE: Unsigned change orders are a leading cause of vendor disputes. The 10-business-day impact assessment window protects Client from Vendor beginning unauthorized work; the requirement for signed Change Orders prevents verbal agreements from expanding scope.

2.4 Key Personnel

- 2.4.1** Vendor shall not replace or reassign Key Personnel without Client's prior written consent, which shall not be unreasonably withheld. Vendor shall provide at least thirty (30) days' prior written notice of any proposed replacement of Key Personnel, together with a proposed replacement's qualifications for Client's review and approval.

- 2.4.2** If Key Personnel become unavailable due to resignation, illness, or other circumstances outside Vendor's control, Vendor shall promptly notify Client and shall propose a qualified replacement within fifteen (15) business days. Client may reject a proposed replacement for reasonable cause.

2.5 Client Cooperation

- 2.5.1** Client shall provide reasonable cooperation, information, and access to Client systems, personnel, and facilities as reasonably required by Vendor to perform the Services. Client's failure to provide such cooperation or access after reasonable notice from Vendor may excuse Vendor's performance to the extent directly caused by such failure, provided Vendor has notified Client in writing and Client has not cured within a reasonable period.
- 2.5.2** Client's cooperation obligations shall not require Client to compromise its own security controls, disclose Confidential Information beyond what is reasonably necessary, or grant access beyond the minimum necessary for Vendor to perform the Services.

2.6 Service Levels

- 2.6.1** Where specified in a SOW or in the Service Level Agreement (Exhibit B), Vendor shall meet the service level commitments set forth therein. In the event of a failure to meet any service level, the remedies set forth in the SLA shall apply, which may include service credits.
- 2.6.2** Service credits are the exclusive remedy for SLA failures unless the failure constitutes a material breach. Service credits shall not constitute a waiver of any other rights or remedies Client may have under this Agreement.
- 2.6.3** Vendor shall provide Client with monthly reports on its performance against all service level commitments within ten (10) business days after the end of each calendar month.

ARTICLE 3 – TERM AND TERMINATION

GUIDANCE: Termination provisions are among the most negotiated clauses in any MSA. Key issues: (1) notice periods for termination for convenience (30–90 days is typical); (2) whether cure periods apply to all breaches or only non-payment; (3) what survives termination, particularly data return/destruction obligations. Ensure the termination for cause provision includes insolvency triggers.

3.1 Term

3.1.1 This Agreement shall commence on the Effective Date and shall continue for an initial term of [one (1) year / two (2) years / three (3) years] (the “Initial Term”) unless earlier terminated in accordance with this Article 3. Thereafter, this Agreement shall automatically renew for successive one (1) year periods (each a “Renewal Term” and, together with the Initial Term, the “Term”), unless either Party provides written notice of non-renewal at least ninety (90) days prior to the end of the then-current Term.

3.2 Termination for Cause

3.2.1 Either Party may terminate this Agreement or any SOW, effective upon written notice, if the other Party materially breaches this Agreement and fails to cure such breach within thirty (30) days after receiving written notice describing the breach in reasonable detail; provided that if the breach is not reasonably susceptible to cure within thirty (30) days, the breaching Party shall have an additional thirty (30) days to cure, so long as it commences cure within the initial thirty (30) day period and diligently pursues cure to completion.

3.2.2 Either Party may terminate this Agreement immediately upon written notice if the other Party: (a) becomes insolvent or admits in writing its inability to pay its debts as they become due; (b) makes a general assignment for the benefit of creditors; (c) has a receiver or trustee appointed; (d) files or has filed against it a petition in bankruptcy that is not dismissed within sixty (60) days; or (e) ceases to conduct its business in the ordinary course.

3.2.3 Client may terminate this Agreement or any SOW immediately upon written notice if Vendor: (a) suffers a Data Breach involving Client Data that Vendor fails to promptly contain and remediate; (b) materially violates the IT Security Addendum and fails to cure within fifteen (15) days of notice; (c) engages in fraud, willful misconduct, or criminal conduct; or (d) becomes subject to a regulatory enforcement action that materially impairs Vendor's ability to perform its obligations.

GUIDANCE: Section 3.2.3 gives Client enhanced termination rights for security failures. The 15-day cure period for IT Security Addendum violations (shorter than the general 30-day period) reflects the urgency of security risks. Negotiate whether the 30-day general cure period applies to payment failures — many Vendors want a shorter 10-day cure for non-payment.

3.3 Termination for Convenience

3.3.1 Client may terminate this Agreement or any SOW for convenience upon sixty (60) days' prior written notice to Vendor. In the event of termination for convenience, Client shall pay Vendor for all Services performed and expenses incurred prior to the effective date of termination, plus any non-cancellable commitments made by Vendor in reasonable reliance on this Agreement, provided Vendor uses reasonable efforts to mitigate such costs.

3.3.2 Vendor may terminate this Agreement for convenience upon one hundred twenty (120) days' prior written notice to Client, provided that no SOW then-in-progress shall be terminated pursuant to this Section 3.3.2 unless the Parties mutually agree to an orderly wind-down schedule.

3.4 Effect of Termination

3.4.1 Upon expiration or termination of this Agreement for any reason: (a) all licenses granted hereunder shall immediately terminate; (b) each Party shall promptly return or destroy the other

Party's Confidential Information as directed in writing; (c) Vendor shall promptly return or securely destroy all Client Data in accordance with Section 6.7; (d) Vendor shall provide Client with a certificate of destruction within thirty (30) days confirming the secure destruction of all Client Data; and (e) each Party shall cooperate in good faith to effect an orderly transition of Services.

- 3.4.2** Vendor shall cooperate fully in any transition of the Services to Client or a successor vendor for a period of up to twelve (12) months following notice of termination ("Transition Period"), at rates to be agreed in advance. During the Transition Period, Vendor shall continue to perform all Services at the same level of quality required under this Agreement.

 **GUIDANCE:** *The Transition Period clause is critical for operational continuity. Twelve months is appropriate for complex engagements; six months may suffice for simpler services. Specify transition rates in the relevant SOW or Fee Schedule to avoid disputes at the moment of greatest leverage imbalance.*

3.5 Survival

- 3.5.1** The following provisions shall survive expiration or termination of this Agreement: Article 1 (Definitions); Section 3.4 (Effect of Termination); Article 5 (Confidentiality); Article 6 (Data Protection and Privacy); Article 7 (Intellectual Property); Article 9 (Audit Rights, for a period of three (3) years); Article 10 (Representations and Warranties, with respect to pre-termination acts); Article 11 (Indemnification); Article 12 (Limitation of Liability); Article 18 (Compliance with Laws, with respect to pre-termination acts); and Article 21 (General Provisions).

ARTICLE 4 – FEES, INVOICING, AND PAYMENT

 **GUIDANCE:** The fees article should cross-reference a detailed Fee Schedule (Exhibit C) rather than embedding all pricing. This structure allows pricing updates without amending the entire MSA. Key negotiation points: net-30 vs. net-45 payment terms; interest rate on late payments; whether Vendor can suspend services for non-payment (typically yes, after notice and cure); and price escalation caps for multi-year agreements.

4.1 Fees

- 4.1.1** Client shall pay Vendor the fees set forth in each applicable SOW and in the Fee Schedule attached as Exhibit C (“Fees”). Except as expressly set forth in a SOW, Vendor shall not charge, and Client shall not be obligated to pay, any fees, costs, or expenses not specified in a signed SOW or Change Order.
- 4.1.2** Vendor may increase recurring fees upon not less than ninety (90) days’ prior written notice to Client; provided that no fee increase shall exceed the lesser of (a) [five percent (5%)] per annum or (b) the percentage change in the Consumer Price Index for All Urban Consumers (CPI-U) for the twelve (12) month period ending in the most recent December. Fee increases above such cap require Client’s prior written consent.

4.2 Invoicing

- 4.2.1** Vendor shall issue invoices in accordance with the invoicing schedule set forth in the applicable SOW. Each invoice shall include: (a) the Agreement number and SOW number; (b) an itemized description of the Services performed; (c) the period covered by the invoice; (d) any applicable taxes; and (e) payment instructions.
- 4.2.2** Vendor shall submit invoices to Client’s designated billing contact by email or through Client’s designated invoicing portal. Invoices that do not comply with the requirements of Section 4.2.1 shall be deemed not received until resubmitted in compliant form.

4.3 Payment Terms

- 4.3.1** Client shall pay all undisputed invoices within thirty (30) days of receipt (“Payment Due Date”). Overdue amounts shall bear interest at the lesser of one and one-half percent (1.5%) per month or the maximum rate permitted by applicable law, calculated from the Payment Due Date.
- 4.3.2** If Client disputes any portion of an invoice in good faith, Client shall: (a) pay the undisputed portion by the Payment Due Date; and (b) provide Vendor with written notice of the disputed amount and the basis for the dispute within fifteen (15) business days of invoice receipt. The Parties shall use good faith efforts to resolve payment disputes within thirty (30) days after Vendor’s receipt of Client’s dispute notice.
- 4.3.3** Following written notice to Client and Client’s failure to cure non-payment of undisputed amounts within fifteen (15) days of such notice, Vendor may suspend performance of Services. Any such suspension shall not relieve Vendor of its data protection, confidentiality, or security obligations.

4.4 Taxes

- 4.4.1** All Fees are exclusive of applicable sales, use, value-added, goods and services, and similar transaction taxes (“Transaction Taxes”). Client shall be responsible for all Transaction Taxes imposed on the Services, except for taxes imposed on Vendor’s net income. Vendor shall separately state Transaction Taxes on each invoice. If Client is exempt from Transaction Taxes, Client shall provide Vendor with a valid exemption certificate prior to invoicing.

4.5 Expenses

- 4.5.1** Vendor shall not charge Client for any expenses (including travel, lodging, meals, or equipment) unless pre-approved in writing by Client’s designated project manager and in accordance with Client’s

then-current travel and expense policy. Expenses shall be documented with receipts and invoiced at actual cost without markup.

ARTICLE 5 – CONFIDENTIALITY

 **GUIDANCE:** *The confidentiality article protects each party's non-public information. In TPRM engagements, Client's Confidential Information includes its risk posture, security assessments, vendor lists, and strategic plans. Ensure the definition of Confidential Information captures information disclosed orally as well as in writing, and that the exceptions are precisely drafted. The obligation to notify of compelled disclosure (subpoena, government demand) is critical.*

5.1 Definition

5.1.1 “Confidential Information” means all non-public information disclosed by one Party (the “Disclosing Party”) to the other Party (the “Receiving Party”) in connection with this Agreement, whether disclosed orally, in writing, electronically, or by any other means, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Without limitation, Client's Confidential Information includes Client Data, security assessments and findings, vendor inventories, risk ratings, pricing, and strategic plans; Vendor's Confidential Information includes its proprietary technology, source code, trade secrets, pricing models, and product roadmaps.

5.2 Confidentiality Obligations

- 5.2.1** Each Receiving Party shall: (a) hold the Disclosing Party's Confidential Information in strict confidence using at least the same degree of care it uses to protect its own confidential information, but in no event less than reasonable care; (b) not disclose Confidential Information to any third party without the Disclosing Party's prior written consent; (c) use Confidential Information only for the purposes of performing obligations or exercising rights under this Agreement; and (d) limit access to Confidential Information to those employees, contractors, and advisors who have a need to know and who are bound by confidentiality obligations at least as protective as those in this Article 5.
- 5.2.2** Vendor shall not use Client's Confidential Information to: (a) train AI Systems; (b) benchmark Vendor's products or services; (c) develop competing products or services; or (d) benefit any third party or Vendor's other clients.

 **GUIDANCE:** *Section 5.2.2 is essential in AI-era contracts. Without this clause, a Vendor providing AI-enabled services could use Client's data to improve models that benefit Vendor's other clients. Ensure AI training prohibitions are also addressed in Article 17 (AI-Specific Provisions) and in the IT Security Addendum.*

5.3 Exceptions

5.3.1 Confidentiality obligations under this Article 5 do not apply to information that: (a) is or becomes publicly known through no breach of this Agreement by the Receiving Party; (b) was rightfully known to the Receiving Party prior to disclosure by the Disclosing Party, as evidenced by written records predating the disclosure; (c) is received from a third party without restriction and without breach of any obligation of confidentiality; or (d) was independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information, as evidenced by written records.

5.4 Compelled Disclosure

5.4.1 If the Receiving Party is required by law, court order, or regulatory authority to disclose Confidential Information, the Receiving Party shall: (a) provide the Disclosing Party with prompt prior written notice to the extent legally permissible; (b) cooperate with the Disclosing Party in seeking a protective order or other appropriate relief; and (c) disclose only the minimum amount of Confidential Information legally required. Disclosure pursuant to this Section 5.4 shall not affect the Receiving Party's other obligations under this Article 5.

5.5 Return and Destruction

5.5.1 Upon expiration or termination of this Agreement, or upon the Disclosing Party's written request, the Receiving Party shall promptly return or destroy all Confidential Information and all copies thereof, and shall certify in writing to the Disclosing Party that it has done so within fifteen (15) business days. Notwithstanding the foregoing, the Receiving Party may retain Confidential Information to the extent required by applicable law, provided that it notifies the Disclosing Party and continues to protect such information in accordance with this Article 5.

5.6 Remedies

5.6.1 Each Party acknowledges that breach of this Article 5 would cause irreparable harm for which monetary damages would be inadequate, and that the non-breaching Party shall be entitled to seek injunctive or other equitable relief without the requirement to post a bond or prove actual damages, in addition to all other remedies available at law or in equity.

ARTICLE 6 – DATA PROTECTION AND PRIVACY

 **GUIDANCE:** This is one of the most complex and rapidly evolving areas of vendor contract law. The Data Processing Agreement (Exhibit E) should carry the bulk of GDPR/CCPA-specific obligations; this article sets the overarching framework. Key issues: purpose limitation (what can Vendor do with Client Data?), subprocessor approval, data subject rights support, cross-border transfer mechanisms, AI-specific data governance, and the data deletion certificate at offboarding.

6.1 Data Processing Agreement

6.1.1 To the extent Vendor processes Personal Data on behalf of Client, Vendor agrees to the terms of the Data Processing Agreement attached as Exhibit E, which is hereby incorporated by reference. In the event of a conflict between this Article 6 and Exhibit E, Exhibit E shall govern with respect to the processing of Personal Data.

6.2 Data Ownership and Purpose Limitation

6.2.1 As between the Parties, Client retains all right, title, and interest in and to Client Data. Vendor acquires no rights in Client Data other than the limited right to use Client Data to perform the Services in accordance with this Agreement and Client's documented instructions.

6.2.2 Vendor shall process Client Data solely: (a) as necessary to perform the Services; (b) in accordance with Client's documented instructions; and (c) as required by applicable law. Vendor shall promptly notify Client if it receives instructions that, in Vendor's reasonable opinion, would violate applicable Privacy Laws.

6.2.3 Vendor shall not: (a) sell, rent, or lease Client Data to any third party; (b) use Client Data for Vendor's own commercial purposes; (c) combine Client Data with data from Vendor's other clients except as expressly authorized in writing; (d) use Client Data for benchmarking or competitive intelligence; or (e) disclose Client Data to law enforcement or government authorities except as required by applicable law and subject to the notice requirements of Section 5.4.

6.3 Data Security

6.3.1 Vendor shall implement and maintain a comprehensive information security program meeting the requirements set forth in the IT Security Addendum (Exhibit D). Such program shall include, at minimum, administrative, technical, and physical safeguards designed to: (a) ensure the security, confidentiality, integrity, and availability of Client Data; (b) protect against anticipated threats or hazards to the security of Client Data; and (c) prevent unauthorized access to or use of Client Data.

6.4 Data Subject Rights

6.4.1 Vendor shall assist Client in responding to data subject rights requests under applicable Privacy Laws (including requests to access, rectify, erase, restrict processing of, or port Personal Data) by implementing appropriate technical and organizational measures. Vendor shall notify Client within five (5) business days of receiving a data subject request that relates to Client Data, and shall not respond to such request without Client's prior written authorization except as required by applicable law.

6.5 Subprocessors

6.5.1 Vendor shall not engage any Subprocessor to process Client Data without Client's prior written approval. Approved Subprocessors as of the Effective Date are listed in Exhibit F. Vendor shall provide at least thirty (30) days' prior written notice of any proposed addition or replacement of a Subprocessor. Client may object to a proposed Subprocessor within twenty (20) days of receiving notice by providing written notice stating the reasonable grounds for objection. If Client objects, the Parties shall work in good faith to resolve the objection; if the Parties cannot resolve the objection within fifteen (15) days, Client may terminate the affected SOW without penalty.

6.5.2 Vendor shall impose data protection obligations on each Subprocessor at least as protective as those applicable to Vendor under this Agreement and applicable Privacy Laws, and shall remain fully liable to Client for the acts and omissions of its Subprocessors.

 **GUIDANCE:** *The subprocessor approval right is a core GDPR requirement for controller-processor relationships. In practice, Vendors often request a general written authorization for a list of Subprocessors and the right to update with 30-day notice and an objection right. The termination-without-penalty provision upon unresolved objection is the essential client protection.*

6.6 Cross-Border Data Transfers

6.6.1 Vendor shall not transfer Client Data outside the country or jurisdiction in which it was collected, or outside the European Economic Area (EEA) or United Kingdom, without Client's prior written consent and the implementation of an appropriate transfer mechanism under applicable Privacy Laws (including, as applicable, Standard Contractual Clauses, an adequacy decision, or other legally recognized mechanism).

6.7 Data Return and Destruction

6.7.1 Upon expiration or termination of this Agreement, or at Client's request at any time, Vendor shall within thirty (30) days: (a) make all Client Data available to Client in a commonly used, machine-readable format; (b) securely delete and destroy all Client Data in Vendor's possession, custody, or control, including all copies, backups, and archives, unless retention is required by applicable law; and (c) certify in writing to Client that all Client Data has been returned and destroyed, specifying the destruction method used.

6.7.2 With respect to AI Systems operated by Vendor: Vendor shall, upon request, use commercially reasonable efforts to ensure that Client Data is removed from AI training datasets, and shall not use Client Data for model training, fine-tuning, or reinforcement learning beyond the scope expressly authorized in writing by Client.

 **GUIDANCE:** *Section 6.7.2 addresses the unique challenge of AI data removal. Complete removal from trained models is technically difficult or impossible; "commercially reasonable efforts" acknowledges this while still creating an obligation. Consider adding a representation that Vendor will not use Client Data for training without affirmative opt-in consent.*

6.8 Privacy Impact Assessments

6.8.1 Vendor shall cooperate with Client in conducting Data Protection Impact Assessments (DPIAs) or Privacy Impact Assessments (PIAs) as required by applicable Privacy Laws or Client's internal policies, providing all information reasonably requested by Client regarding Vendor's data processing activities.

ARTICLE 7 – INTELLECTUAL PROPERTY

 **GUIDANCE:** IP ownership is often the most contentious negotiation in professional services agreements. The default rule is that Vendor retains IP created in the course of services unless the agreement says otherwise. For TPRM engagements, Client should own all Deliverables and reports specific to its risk environment. Generic methodologies and tools developed by Vendor remain Vendor's Background IP. AI-generated outputs create novel IP questions: document ownership expectations clearly.

7.1 Background IP

7.1.1 Each Party retains all right, title, and interest in its Background IP. Nothing in this Agreement transfers ownership of, or grants any rights in, either Party's Background IP except as expressly set forth herein.

7.1.2 Vendor hereby grants Client a limited, non-exclusive, non-transferable, royalty-free license to use Vendor's Background IP solely to the extent incorporated into Deliverables and solely for Client's internal business purposes in connection with the Services.

7.2 Work Product Ownership

7.2.1 Except as set forth in Section 7.1, all Work Product created by Vendor specifically for Client under this Agreement shall be and remain the exclusive property of Client. To the extent Work Product qualifies as a "work made for hire" under applicable copyright law, it shall be deemed a work made for hire. To the extent Work Product does not qualify as a work made for hire, Vendor hereby irrevocably assigns to Client all right, title, and interest in and to such Work Product, including all Intellectual Property Rights therein.

7.2.2 Vendor shall execute any documents and take any actions reasonably requested by Client to evidence, perfect, or enforce Client's ownership of Work Product.

7.3 Pre-Existing Vendor Technology and Tools

7.3.1 Any pre-existing Vendor technology, tools, templates, methodologies, or other materials incorporated into Work Product shall remain Vendor's property. Vendor grants Client a perpetual, irrevocable, royalty-free, non-exclusive license to use such pre-existing materials as incorporated into Work Product for Client's internal business purposes.

7.4 AI-Generated Work Product

7.4.1 If Vendor uses AI Systems to generate or assist in generating Work Product: (a) Vendor shall disclose such use to Client in writing; (b) Vendor shall represent that it has the rights necessary to assign or license AI-generated outputs to Client; (c) Client's ownership of such AI-generated Work Product is subject to applicable law regarding AI-generated works, and Vendor makes no warranty that such outputs are protectable by copyright or other Intellectual Property Rights; and (d) Vendor shall not use Client Data or Confidential Information as input to third-party AI Systems without Client's prior written consent.

 **GUIDANCE:** AI-generated work IP is an unsettled area of law. The U.S. Copyright Office has held that purely AI-generated content with no human creative input is not protectable by copyright. Require Vendor to disclose AI tool use and indemnify Client for third-party IP claims arising from Vendor's use of AI tools with Client data.

7.5 No Implied Licenses

7.5.1 Except as expressly set forth in this Agreement, neither Party grants the other any license, right, title, or interest in any Intellectual Property Rights by implication, estoppel, or otherwise.

7.6 Open Source Software

- 7.6.1** Vendor shall not incorporate any open source or third-party software into Deliverables that would:
- (a) require Client to disclose or distribute any of its proprietary source code; (b) create any lien, obligation, or encumbrance on Client's proprietary software or IP; or (c) grant any third party any rights in Client's proprietary software or IP. Vendor shall provide Client with a complete list of all open source components incorporated into Deliverables, together with applicable license terms, upon request.

ARTICLE 8 – SECURITY

 **GUIDANCE:** *This article cross-references the IT Security Addendum (Exhibit D) as the operative security document. The IT Security Addendum can be updated as the threat landscape evolves without amending the full MSA. Key provisions here: the right to update security requirements over the Term; Vendor's obligation to inform Client of security changes; and the right to conduct security assessments.*

- 8.1** Vendor shall at all times during the Term maintain and comply with the information security requirements set forth in the IT Security Addendum (Exhibit D). The IT Security Addendum is incorporated into this Agreement by reference.
- 8.2** Client reserves the right to update the IT Security Addendum to address evolving threats, new regulatory requirements, or changes in industry standards, upon not less than sixty (60) days' written notice to Vendor. If compliance with an updated IT Security Addendum would impose material additional costs on Vendor, the Parties shall negotiate in good faith a fee adjustment or, if no agreement is reached within thirty (30) days, either Party may terminate the affected SOW upon ninety (90) days' notice.
- 8.3** Vendor shall promptly notify Client of any material change to Vendor's security controls, certifications, or practices that may affect Vendor's ability to comply with the IT Security Addendum, and shall not make such changes without Client's prior written approval where the change would reduce Vendor's security posture with respect to Client Data.
- 8.4** Vendor shall not introduce Malicious Code into any Client system, network, or environment. Vendor shall maintain current anti-malware controls on all systems used to deliver the Services or access Client Data.

ARTICLE 9 – AUDIT RIGHTS

 **GUIDANCE:** *Audit rights are essential for TPRM but are often heavily negotiated. Vendors resist on-site audits as disruptive and costly; Clients need meaningful verification of compliance. A balanced approach: accept third-party audit reports (SOC 2 Type II, ISO 27001) as the primary evidence mechanism, with on-site rights reserved for material concerns. Ensure audit rights cover subprocessors. Add a questionnaire right (annual, at minimum) as a lower-cost complement to formal audits.*

- 9.1** Client shall have the right, no more than once per calendar year and upon at least thirty (30) days' prior written notice, to audit Vendor's compliance with this Agreement, including Vendor's security controls, data protection practices, and financial records relevant to the Services. Audits shall be conducted during normal business hours in a manner that minimizes disruption to Vendor's operations. Each Party shall bear its own costs for audits conducted pursuant to this Section; provided that if an audit reveals a material breach, Vendor shall bear Client's reasonable audit costs.
- 9.2** In lieu of or in addition to an on-site audit, Client may request that Vendor provide: (a) a copy of Vendor's most recent SOC 2 Type II or comparable audit report within thirty (30) days of issuance; (b) responses to Client's information security questionnaire on an annual basis; and (c) evidence of current security certifications (including ISO/IEC 27001, PCI-DSS, or as applicable).
- 9.3** In the event of a Data Breach or a reasonable suspicion of a material security failure, Client may conduct an additional unscheduled audit upon forty-eight (48) hours' notice, or such shorter period as the circumstances require. Vendor shall cooperate fully with any such audit and shall not deny or obstruct Client's access to relevant systems, records, or personnel.
- 9.4** Audit rights under this Article 9 extend to Vendor's Subprocessors that process Client Data. Vendor shall include equivalent audit rights for Client (directly or through Vendor) in all Subprocessor agreements.
- 9.5** All information obtained by Client during an audit is the Confidential Information of Vendor and shall be used by Client solely to verify compliance with this Agreement.

ARTICLE 10 – REPRESENTATIONS AND WARRANTIES

 **GUIDANCE:** Representations and warranties allocate risk by ensuring each party has made the statements that induced the other to enter the agreement. Vendor's warranties should include: (1) authority to enter the agreement; (2) no conflicting obligations; (3) performance conforming to specifications; (4) no malicious code; (5) no infringement; and (6) compliance with law. Client's warranties are typically narrower. Survival periods for warranties should be specified.

10.1 Mutual Representations and Warranties

Each Party represents and warrants to the other that, as of the Effective Date and throughout the Term:

- 10.1.1 it is a legal entity duly organized, validly existing, and in good standing under the laws of its jurisdiction of formation;
- 10.1.2 it has full corporate power and authority to enter into this Agreement and to perform its obligations hereunder;
- 10.1.3 this Agreement has been duly authorized by all necessary corporate action and constitutes a legal, valid, and binding obligation, enforceable against it in accordance with its terms;
- 10.1.4 execution, delivery, and performance of this Agreement do not violate any applicable law, regulation, court order, or agreement to which it is a party or by which it is bound; and
- 10.1.5 it is not a party to, and has not received notice of, any legal proceeding that would materially impair its ability to perform its obligations under this Agreement.

10.2 Vendor Representations and Warranties

Vendor represents and warrants to Client that, as of the Effective Date and throughout the Term:

- 10.2.1 the Services will be performed in a professional and workmanlike manner, consistent with industry standards, and will conform in all material respects to the specifications set forth in the applicable SOW;
- 10.2.2 Vendor has and will maintain all licenses, permits, certifications, and authorizations required to perform the Services;
- 10.2.3 the Services, Deliverables, and Vendor's Background IP, as used in the performance of the Services, will not infringe, misappropriate, or violate any third party's Intellectual Property Rights;
- 10.2.4 Vendor will not introduce, and will take commercially reasonable steps to prevent the introduction of, Malicious Code into any Client system, environment, or data;
- 10.2.5 Vendor's security program, as of the Effective Date and throughout the Term, meets or exceeds the requirements of the IT Security Addendum;
- 10.2.6 Vendor will comply with all applicable laws and regulations in the performance of the Services, including Privacy Laws;
- 10.2.7 Vendor has implemented, and will maintain throughout the Term, a comprehensive and industry-standard information security program, as further described in the IT Security Addendum;
- 10.2.8 no Key Personnel assigned to Client's account is, to Vendor's knowledge, subject to any pending criminal proceedings or regulatory actions that would impair such person's ability to perform the Services; and
- 10.2.9 all information and documentation provided by Vendor to Client in connection with Client's due diligence of Vendor, including security questionnaire responses, audit reports, and certifications, is accurate and complete in all material respects as of the date provided.

10.3 Disclaimer of Warranties

10.3 EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AND TITLE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

ARTICLE 11 – INDEMNIFICATION

 **GUIDANCE:** Indemnification clauses allocate litigation defense costs and damages to the party whose acts gave rise to a claim. Mutual indemnification is standard for general negligence and IP infringement. Data breach and privacy violation indemnification should be one-way (Vendor to Client) unless Client controls data processing. Ensure Client's IP indemnification covers scenarios where Vendor uses Client materials per Client's instructions. The notice-and-cooperation clause is essential: failure to timely notify can forfeit indemnity rights.

11.1 Vendor Indemnification

11.1.1 Vendor shall indemnify, defend, and hold harmless Client and its officers, directors, employees, agents, successors, and assigns (“Client Indemnitees”) from and against any and all claims, demands, suits, proceedings, losses, damages, liabilities, costs, and expenses (including reasonable attorneys’ fees) (“Losses”) arising out of or related to:

- (a) any breach or alleged breach by Vendor of its representations, warranties, or obligations under this Agreement;
- (b) Vendor’s or its Subcontractors’ negligence, fraud, willful misconduct, or violation of applicable law;
- (c) any claim that the Services, Deliverables, or Vendor’s Background IP infringes or misappropriates any third party’s Intellectual Property Rights, provided that Client has not modified the allegedly infringing materials or combined them with other materials in a manner that creates the infringement;
- (d) any Data Breach caused by Vendor’s failure to comply with its security obligations, including all costs of investigation, notification, remediation, regulatory response, credit monitoring services, and regulatory fines attributable to Vendor’s failure; and
- (e) any violation of applicable Privacy Laws by Vendor in connection with its processing of Client Data.

11.2 Client Indemnification

11.2.1 Client shall indemnify, defend, and hold harmless Vendor and its officers, directors, employees, agents, successors, and assigns (“Vendor Indemnitees”) from and against any Losses arising out of or related to:

- (a) any breach by Client of its representations, warranties, or obligations under this Agreement;
- (b) Client’s negligence, fraud, or willful misconduct; and
- (c) any claim that Client Materials (data, software, or other materials provided by Client to Vendor for use in the Services) infringe or misappropriate any third party’s Intellectual Property Rights.

11.3 Indemnification Procedure

11.3.1 The Party seeking indemnification (“Indemnified Party”) shall: (a) promptly notify the indemnifying Party (“Indemnifying Party”) in writing of any claim for which indemnification is sought, provided that failure to timely notify shall not relieve the Indemnifying Party of its obligations except to the extent the Indemnifying Party is materially prejudiced by such failure; (b) grant the Indemnifying Party sole control of the defense and settlement of the claim; and (c) provide reasonable cooperation and assistance to the Indemnifying Party at the Indemnifying Party’s expense.

11.3.2 The Indemnifying Party shall not settle any claim in a manner that imposes any obligation, restriction, or liability on the Indemnified Party, or that does not include a full release of the Indemnified Party, without the Indemnified Party’s prior written consent.

11.3.3 The Indemnified Party retains the right to participate in the defense of any claim at its own expense with counsel of its own choosing.

ARTICLE 12 – LIMITATION OF LIABILITY

GUIDANCE: Limitation of liability is the most aggressively negotiated provision in any technology services agreement. Key issues: (1) What is the cap? Typically 12 months of fees paid; for high-risk engagements consider 24–36 months or unlimited for data breaches; (2) What is excluded from the cap (carve-outs)? Data breaches, willful misconduct, death/bodily injury, and IP indemnification commonly are carved out; (3) Mutual or one-way? Caps are typically mutual. Consider a higher sub-cap specifically for data breach liability.

12.1 LIMITATION ON INDIRECT DAMAGES. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, INCLUDING LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS, OR LOSS OF DATA, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; PROVIDED, HOWEVER, THAT THE FOREGOING SHALL NOT LIMIT VENDOR'S LIABILITY FOR: (A) DATA BREACHES INVOLVING CLIENT DATA; (B) VENDOR'S VIOLATION OF ITS CONFIDENTIALITY OBLIGATIONS; (C) VENDOR'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT; OR (D) VENDOR'S INDEMNIFICATION OBLIGATIONS UNDER ARTICLE 11.

12.2 CAP ON LIABILITY. EXCEPT FOR THE CARVE-OUTS LISTED IN SECTION 12.3, EACH PARTY'S AGGREGATE LIABILITY TO THE OTHER PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT SHALL NOT EXCEED THE GREATER OF (A) THE TOTAL FEES PAID OR PAYABLE BY CLIENT TO VENDOR IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM, OR (B) [USD \$_____].

12.3 CARVE-OUTS. THE LIABILITY CAP SET FORTH IN SECTION 12.2 SHALL NOT APPLY TO: (A) EITHER PARTY'S INDEMNIFICATION OBLIGATIONS FOR THIRD-PARTY IP CLAIMS UNDER ARTICLE 11; (B) VENDOR'S DATA BREACH LIABILITY, WHICH SHALL BE SUBJECT TO A SEPARATE SUB-CAP OF [TWO (2) TIMES / THREE (3) TIMES] THE FEES PAID IN THE TWELVE (12) MONTHS PRECEDING THE BREACH; (C) EITHER PARTY'S FRAUD OR WILLFUL MISCONDUCT; (D) VIOLATION OF ARTICLE 5 (CONFIDENTIALITY); OR (E) VENDOR'S VIOLATION OF PRIVACY LAWS WITH RESPECT TO PROCESSING OF CLIENT DATA.

GUIDANCE: The carve-out for data breach liability with a separate sub-cap (2x–3x annual fees) reflects market practice for agreements where Vendor handles sensitive data. The data breach sub-cap should be set at a level sufficient to cover realistic notification, remediation, and regulatory response costs. For very large data sets, consider unlimited liability or a fixed floor amount.

12.4 The Parties acknowledge that the limitations of liability set forth in this Article 12 are a fundamental element of the basis of the bargain between the Parties, and that the Fees reflect the allocation of risk contemplated by these limitations. Each Party has had the opportunity to negotiate these limitations and has found them reasonable.

ARTICLE 13 – INSURANCE

 **GUIDANCE:** Insurance requirements should be tailored to the risk profile of the Services. Cyber/technology E&O coverage is essential for any Vendor handling Client Data. Workers' compensation is required by law in most jurisdictions. Verify that required coverage limits align with the liability cap — it is counterproductive to set a \$10M liability cap but only require \$1M in cyber coverage. Require that Client is listed as additional insured on CGL and auto policies.

- 13.1** Vendor shall obtain and maintain, at its own expense, throughout the Term and for a period of three (3) years thereafter, the following insurance coverages with insurers rated A- or better by A.M. Best:
- (a) Commercial General Liability: not less than USD \$2,000,000 per occurrence and USD \$5,000,000 in the aggregate;
 - (b) Professional Liability / Errors and Omissions: not less than USD \$5,000,000 per claim and in the aggregate;
 - (c) Cyber Liability and Data Breach / Technology Errors and Omissions: not less than USD \$[5,000,000 / 10,000,000] per occurrence and in the aggregate, covering Data Breaches, unauthorized access, privacy regulatory defense and penalties, network security liability, media liability, and crisis management costs;
 - (d) Workers' Compensation: as required by applicable law, plus Employers' Liability of not less than USD \$1,000,000;
 - (e) Commercial Automobile Liability (if applicable): not less than USD \$1,000,000 combined single limit.
- 13.2** Client shall be named as an additional insured on Vendor's Commercial General Liability and Automobile Liability policies. All Vendor policies shall include a waiver of subrogation in favor of Client.
- 13.3** Vendor shall provide Client with certificates of insurance evidencing compliance with this Article 13 within ten (10) business days of execution of this Agreement and annually thereafter, and shall provide at least thirty (30) days' prior written notice of any cancellation or material reduction in coverage.

ARTICLE 14 – SUBCONTRACTORS AND SUBPROCESSORS

 **GUIDANCE:** *Subcontractor and subprocessor management is a core TPRM concern — a Vendor's supply chain is an extension of the Client's risk surface. Key obligations: pre-approval for material subcontractors; flow-down of all MSA obligations (especially security and data protection); Vendor remains fully liable for subcontractor acts; and Client has audit rights extending to subprocessors.*

- 14.1** Vendor shall not subcontract any material portion of the Services or engage any Subprocessor without Client's prior written approval. Approved Subcontractors and Subprocessors as of the Effective Date are listed in Exhibit F.
- 14.2** Vendor shall include in each subcontract provisions that: (a) impose on each Subcontractor obligations consistent with Vendor's obligations under this Agreement, including with respect to confidentiality, data protection, security, IP ownership, and compliance with law; (b) grant Client the right to enforce such obligations directly against the Subcontractor; and (c) require each Subcontractor to comply with the IT Security Addendum.
- 14.3** Vendor shall remain fully responsible and liable to Client for all acts and omissions of its Subcontractors and Subprocessors as if Vendor had performed such acts or omissions directly. The engagement of a Subcontractor shall not relieve Vendor of any of its obligations under this Agreement.
- 14.4** Vendor shall conduct security assessments of all Subcontractors and Subprocessors that will have access to Client Data at least annually and shall provide Client with the results of such assessments upon request. Vendor shall promptly notify Client of any material security finding relating to a Subcontractor or Subprocessor that may affect Client Data.

ARTICLE 15 – BUSINESS CONTINUITY AND DISASTER RECOVERY

 **GUIDANCE:** Business continuity and disaster recovery requirements have become increasingly prominent post-COVID and post-SolarWinds. DORA (EU Digital Operational Resilience Act) and NIST CSF 2.0 both explicitly require organizations to verify vendor BCP/DR capabilities. Key metrics to require: Recovery Time Objective (RTO), Recovery Point Objective (RPO), and annual testing with results available to Client.

- 15.1** Vendor shall maintain a written, board-approved Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) that address the continuity and recovery of all Services in the event of a disruption, disaster, or other emergency. The BCP and DRP shall include, at minimum: (a) documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical Service component; (b) redundant systems and data backup procedures; (c) roles, responsibilities, and contact information for continuity and recovery personnel; (d) communication procedures for notifying Client of disruptions; and (e) escalation procedures.
- 15.2** Vendor's RTO and RPO for all Services covered by a SOW shall be as specified in that SOW or the SLA (Exhibit B). In the absence of specified RTO/RPO, Vendor shall target an RTO of four (4) hours and RPO of one (1) hour for critical systems.
- 15.3** Vendor shall test its BCP and DRP at least annually and shall provide Client with a summary of test results, including any identified gaps and remediation plans, within thirty (30) days of completing each test. Upon request, Client may participate as an observer in Vendor's BCP/DRP testing.
- 15.4** In the event of a disruption to the Services, Vendor shall notify Client within [two (2) / four (4)] hours of Vendor's declaration of a continuity event, and shall provide regular status updates (at least every four (4) hours) until normal operations are restored.

ARTICLE 16 – INCIDENT RESPONSE AND NOTIFICATION

GUIDANCE: Incident response and notification timelines are a regulatory hot-button: GDPR requires notification within 72 hours of becoming aware of a breach; many U.S. state laws require notification within 30–72 hours. A 24-hour contractual notification requirement gives Client time to assess and comply with its own regulatory obligations. The scope of a “Security Incident” should be broad — include suspected incidents, not just confirmed ones.

16.1 Security Incidents

16.1.1 A “Security Incident” means: (a) any unauthorized access to, acquisition, use, disclosure, modification, or destruction of Client Data; (b) any actual or suspected Data Breach; (c) any compromise of Vendor’s systems that could materially affect the security, availability, or integrity of Client Data or the Services; (d) any ransomware, malware, or denial-of-service attack affecting Vendor’s systems that process Client Data; or (e) any unauthorized physical access to facilities where Client Data is processed or stored.

16.2 Incident Detection and Response

16.2.1 Vendor shall maintain incident detection and response capabilities meeting the requirements of the IT Security Addendum, including: (a) continuous monitoring of all systems that process Client Data; (b) documented incident response procedures; (c) a designated incident response team; and (d) the ability to rapidly contain, investigate, and remediate Security Incidents.

16.3 Notification Requirements

16.3.1 Vendor shall notify Client’s designated security contact of any Security Incident without undue delay and in no event later than twenty-four (24) hours after Vendor becomes aware of or reasonably suspects the occurrence of a Security Incident. Initial notification may be oral, followed by written notification within twenty-four (24) hours confirming the oral notification.

16.3.2 The written notification shall include, to the extent then known: (a) the date and time the Security Incident was discovered; (b) a description of the nature of the Security Incident, including the categories and approximate number of individuals and records affected; (c) the likely consequences of the Security Incident; (d) the measures taken or proposed to address the Security Incident and mitigate its effects; (e) the contact information of Vendor’s data protection officer or designated security contact; and (f) whether law enforcement has been notified.

16.3.3 Vendor shall provide Client with regular updates on the investigation and remediation of any Security Incident at intervals requested by Client, and shall cooperate fully with Client’s investigation of any Security Incident.

GUIDANCE: The 24-hour notification requirement is tighter than GDPR’s 72-hour regulator notification window, giving Client time to prepare its own regulatory response. Vendors typically push back on this; 48 hours is a common compromise. Consider including a hotline number or dedicated email for security notifications that is monitored 24/7.

16.4 Remediation

16.4.1 Following a Security Incident, Vendor shall: (a) promptly take all reasonable steps to contain and mitigate the Security Incident; (b) conduct or commission a forensic investigation and provide Client with the full investigation report within thirty (30) days of the Security Incident being contained; (c) implement all remediation measures identified in the investigation report; (d) provide Client with a written remediation plan within fifteen (15) days of the investigation report, with committed timelines for each remediation action; and (e) provide Client with a root cause analysis.

16.4.2 Vendor shall bear all costs associated with investigating, containing, remediating, and notifying affected individuals of any Security Incident caused by Vendor’s breach of its security obligations.

16.5 Regulatory Cooperation

16.5.1 Vendor shall cooperate fully with Client in responding to any regulatory inquiry, investigation, or enforcement action arising from a Security Incident. Vendor shall not communicate with any regulatory authority regarding Client Data without Client's prior written consent, except where Vendor is legally required to do so, in which case Vendor shall notify Client as soon as practicable and shall provide Client with copies of all such communications.

ARTICLE 17 – AI-SPECIFIC PROVISIONS

GUIDANCE: *AI-specific contract provisions are still evolving but are increasingly required by regulators. The EU AI Act (effective 2025–2026) imposes specific obligations on deployers of high-risk AI systems. NIST AI RMF and ISO/IEC 42001 provide governance frameworks. Key issues: (1) AI tool disclosure and approval; (2) prohibition on using Client Data for training; (3) explainability requirements; (4) bias detection and remediation; (5) model drift monitoring; and (6) liability for AI errors. This article should be supplemented by the IT Security Addendum's AI security requirements.*

17.1 AI Tool Disclosure and Approval

17.1.1 Vendor shall disclose to Client, prior to deployment, all AI Systems used in the performance of the Services or that will process Client Data. Vendor shall obtain Client's prior written approval before deploying any new AI System in connection with the Services or making material changes to an approved AI System.

17.1.2 Vendor shall maintain and provide to Client upon request an AI System inventory listing all AI Systems used in the Services, including: (a) the name and version of each AI System; (b) the AI System's intended use and the Services component it supports; (c) the AI System developer and any relevant third-party providers; (d) data inputs processed by the AI System; (e) known limitations; and (f) applicable regulatory classification (e.g., EU AI Act risk tier).

17.2 Prohibition on Training with Client Data

17.2.1 Vendor shall not use Client Data, Confidential Information, or any data derived therefrom to train, fine-tune, retrain, or otherwise improve any AI System, including any third-party AI model, without Client's express prior written consent. This prohibition applies to all AI Systems used by Vendor, including those provided by third parties.

17.2.2 Vendor shall implement technical and organizational measures to prevent Vendor personnel from inputting Client Data or Confidential Information into unauthorized AI Systems or tools, including commercially available generative AI tools not approved under Section 17.1.1.

GUIDANCE: *Section 17.2.2 addresses "Shadow AI" — employees using unauthorized AI tools (e.g., free tiers of ChatGPT, Claude, Gemini) that may retain inputs for training. This is a leading emerging risk in TPRM. Complement with a policy requirement: Vendor must have a written Acceptable Use Policy for AI tools that addresses data entry prohibitions.*

17.3 Explainability and Transparency

17.3.1 Where AI Systems are used to make or support decisions that materially affect Client or Client's customers, Vendor shall provide Client with: (a) a plain-language explanation of how the AI System operates and the basis for its outputs; (b) documentation of the AI System's training data sources, known limitations, and potential biases; and (c) upon request, an explanation of the basis for any specific AI-generated decision or recommendation.

17.4 Bias, Fairness, and Non-Discrimination

17.4.1 Vendor shall implement and document processes to identify, assess, and mitigate bias in AI Systems used in the Services, particularly where those AI Systems make or support decisions affecting individuals. Vendor shall provide Client with the results of its bias assessments upon request and shall remediate identified bias within a timeframe agreed with Client.

17.5 Model Drift and Performance Monitoring

17.5.1 Vendor shall monitor the performance of all AI Systems used in the Services on an ongoing basis and shall promptly notify Client of: (a) any material degradation in AI System performance; (b)

significant model drift or changes in AI System behavior; (c) any AI System update, retraining, or replacement; and (d) any new or materially changed limitations or risks identified through monitoring.

17.6 EU AI Act Compliance

17.6.1 To the extent any AI System used in the Services is subject to the EU AI Act, Vendor shall: (a) classify each such AI System in accordance with the Act's risk categories; (b) comply with all applicable obligations for the relevant risk tier; (c) maintain a conformity assessment and technical documentation as required; and (d) cooperate with Client in meeting Client's obligations as a deployer of high-risk AI Systems, including human oversight requirements, log maintenance, and transparency to affected individuals.

17.7 Liability for AI Errors

17.7.1 Vendor shall not use the involvement of an AI System as a defense to or limitation of its liability for inaccurate, biased, or otherwise defective outputs that cause harm to Client. Vendor's standard of care for AI-driven Services is the same as for any other Services.

ARTICLE 18 – COMPLIANCE WITH LAWS

 **GUIDANCE:** *A general compliance clause is a catch-all. For regulated industries, supplement with a sector-specific exhibit listing all applicable regulations (HIPAA for healthcare, GLBA for financial services, ITAR/EAR for defense, FedRAMP for government). The anti-corruption and sanctions clauses are increasingly required by compliance programs and insurers.*

- 18.1** Each Party shall comply with all applicable federal, state, local, and international laws, regulations, orders, and directives applicable to its performance under this Agreement, including without limitation Privacy Laws, cybersecurity regulations, export control laws, anti-corruption laws (including the FCPA and UK Bribery Act), economic sanctions regulations (including OFAC), anti-money laundering laws, and applicable employment and labor laws.
- 18.2** Vendor shall maintain a written compliance program that includes, at minimum: (a) a code of conduct; (b) anti-corruption and anti-bribery policies; (c) data protection and privacy policies; (d) an AI acceptable use policy; (e) a security incident response policy; and (f) an employee training program covering each of the foregoing. Vendor shall provide evidence of such program to Client upon request.
- 18.3** Vendor shall promptly notify Client of any: (a) regulatory investigation, enforcement action, or inquiry directed at Vendor that relates to the Services or Client Data; (b) material violation by Vendor of applicable law that may affect Vendor's ability to perform the Services; or (c) changes in applicable law of which Vendor becomes aware that may affect Vendor's or Client's obligations under this Agreement.
- 18.4** Vendor represents and warrants that neither it nor any of its officers, directors, employees, or agents has been: (a) debarred or suspended from contracting with any governmental authority; (b) subject to sanctions by OFAC or any comparable authority; or (c) convicted of any crime involving fraud, corruption, or dishonesty. Vendor shall promptly notify Client if any of the foregoing representations ceases to be accurate.

ARTICLE 19 – FORCE MAJEURE

 **GUIDANCE:** Force majeure clauses have been heavily litigated since COVID-19. Key drafting issues: (1) cyber attacks are NOT a force majeure event for a security vendor — that is precisely the risk they are being paid to manage; (2) notice periods matter; (3) Client's right to terminate if the force majeure event persists for an extended period (30–60 days) protects Client from indefinite suspension of Services.

- 19.1** Neither Party shall be in breach of this Agreement or liable for delay in performing, or failure to perform, any obligation under this Agreement to the extent such delay or failure results from a Force Majeure Event. A “Force Majeure Event” means any event beyond a Party’s reasonable control that could not have been anticipated or prevented by the exercise of reasonable diligence, including: acts of God, natural disasters, war, terrorism, civil unrest, strikes or labor disputes not involving the affected Party’s employees, epidemic or pandemic, or governmental actions or orders.
- 19.2** Force Majeure Events expressly do not include: (a) failures of Vendor’s IT infrastructure, systems, or software, unless caused by a broader event meeting the definition of Force Majeure Event; (b) cyber attacks or Security Incidents, which are foreseeable risks that Vendor is obligated to manage under this Agreement; (c) supply chain or staffing shortages that are foreseeable or that should have been mitigated by reasonable contingency planning; or (d) financial difficulty of Vendor.
- 19.3** The Party claiming Force Majeure shall promptly notify the other Party in writing (and in no event more than twenty-four (24) hours after the commencement of the event), describing the event, its likely duration, and the steps being taken to mitigate its effects.
- 19.4** If a Force Majeure Event affecting Vendor’s performance continues for more than thirty (30) consecutive days, Client may terminate the affected SOW or this Agreement upon written notice, without liability to Vendor other than payment for Services performed prior to the Force Majeure Event.

ARTICLE 20 – DISPUTE RESOLUTION

 **GUIDANCE:** *An escalation ladder (business contacts → senior executives → mediation → arbitration/litigation) reduces litigation costs. For B2B technology services, arbitration before JAMS or AAA (or ICC for international agreements) is common. Ensure governing law and venue are specified. The Parties should be free to seek equitable relief (injunctions) in any court of competent jurisdiction without exhausting the dispute resolution process.*

- 20.1** In the event of any dispute arising out of or related to this Agreement (a “Dispute”), the Parties shall first attempt to resolve the Dispute through good faith negotiation between their respective designated project managers within fifteen (15) business days of written notice of the Dispute.
- 20.2** If the Dispute is not resolved pursuant to Section 20.1, either Party may escalate the Dispute to the Parties’ respective senior executives (VP level or above) for further good faith negotiation for an additional fifteen (15) business days.
- 20.3** If the Dispute is not resolved pursuant to Section 20.2, the Parties may, by mutual agreement, submit the Dispute to non-binding mediation administered by [JAMS / AAA / agreed mediator] before initiating arbitration or litigation.
- 20.4** Any Dispute not resolved through the procedures set forth in Sections 20.1 through 20.3 shall be finally resolved by binding arbitration administered by [JAMS / AAA] in accordance with its then-current [Commercial Arbitration Rules / Comprehensive Arbitration Rules and Procedures]. The arbitration shall be conducted by [one arbitrator / three arbitrators] in [City, State]. The arbitration award may be entered as a judgment in any court of competent jurisdiction.
- 20.5** Notwithstanding the foregoing, either Party may seek emergency equitable relief (including temporary restraining orders and preliminary injunctions) in any court of competent jurisdiction to prevent irreparable harm pending the outcome of the dispute resolution process.
- 20.6** This Agreement shall be governed by and construed in accordance with the laws of the State of [Delaware / New York / other], without regard to its conflict of law principles.

ARTICLE 21 – GENERAL PROVISIONS

 **GUIDANCE:** General provisions are often treated as boilerplate but contain critical provisions. Anti-assignment: Client should be able to assign to an Affiliate or in an M&A transaction without Vendor consent. Entire agreement: ensures prior negotiations do not bind the Parties. Amendment: changes must be in writing and signed. Notice: specify email notice is acceptable for operational notices but registered mail is required for termination and legal notices.

21.1 Entire Agreement

This Agreement, together with all Exhibits and SOWs, constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior agreements, representations, and understandings, whether oral or written, relating to such subject matter. No terms or conditions in any purchase order, acknowledgment, or other document issued by Client shall alter the terms of this Agreement unless expressly agreed to in writing by Vendor.

21.2 Amendment

This Agreement may not be amended or modified except by a written instrument signed by authorized representatives of both Parties.

21.3 Waiver

No failure or delay by either Party to exercise any right or remedy under this Agreement shall constitute a waiver of such right or remedy. No single or partial exercise of any right or remedy shall preclude any further exercise of such right or remedy.

21.4 Assignment

Neither Party may assign or transfer this Agreement or any of its rights or obligations hereunder without the other Party's prior written consent, except that: (a) Client may assign this Agreement without consent to an Affiliate or in connection with a merger, acquisition, or sale of all or substantially all of Client's assets, provided that the assignee agrees in writing to be bound by the terms of this Agreement; and (b) Vendor may assign this Agreement without consent to an Affiliate, provided that Vendor remains liable for its obligations hereunder and gives Client thirty (30) days' prior written notice. Any purported assignment in violation of this Section is void.

21.5 Notices

All notices required or permitted under this Agreement shall be in writing and shall be delivered by: (a) personal delivery; (b) nationally recognized overnight courier; (c) registered or certified mail, return receipt requested, postage prepaid; or (d) email with confirmation of receipt (for operational notices only, not for notices of termination, breach, or legal process). Notices shall be addressed to the contacts designated in the applicable SOW or as updated by a Party in writing.

21.6 Severability

If any provision of this Agreement is held invalid, illegal, or unenforceable, such provision shall be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions shall continue in full force and effect.

21.7 Counterparts and Electronic Signatures

This Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same instrument. Electronic signatures (including PDF and DocuSign) shall be deemed valid and binding to the same extent as original signatures.

21.8 Relationship of the Parties

The Parties are independent contractors. Nothing in this Agreement creates a partnership, joint venture, employment, or agency relationship between the Parties. Neither Party has authority to bind the other Party to any obligation.

21.9 No Third-Party Beneficiaries

This Agreement is for the sole benefit of the Parties and their respective permitted successors and assigns. Nothing in this Agreement shall create or be deemed to create any right in or for any third party.

21.10 Export Controls

Each Party shall comply with all applicable export control laws and regulations, including those of the United States (including the Export Administration Regulations and OFAC regulations) and any other applicable jurisdiction. Neither Party shall export or re-export any Services, software, or technical data in violation of such laws.

21.11 Publicity

Neither Party shall issue any press release, public announcement, or other public communication regarding this Agreement or the relationship between the Parties without the other Party's prior written consent. Vendor shall not use Client's name, logo, or trademarks in any marketing materials without Client's prior written consent.

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties have executed this Master Services Agreement as of the Effective Date.

[CLIENT LEGAL NAME]	[VENDOR LEGAL NAME]
Signature	Signature
Printed Name	Printed Name
Title	Title
Date	Date

EXHIBIT A

STATEMENT OF WORK

Each Statement of Work shall describe the specific Services, Deliverables, timeline, fees, Key Personnel, Client responsibilities, and applicable service levels for a discrete engagement. A separate Exhibit A shall be attached for each SOW executed under this Agreement, numbered sequentially (Exhibit A-1, Exhibit A-2, etc.).

EXHIBIT B

SERVICE LEVEL AGREEMENT

The Service Level Agreement shall specify measurable performance commitments for the Services, including uptime, response times, resolution times, and associated service credit formulas. SLA metrics shall be tailored to the specific Services in each Statement of Work.

EXHIBIT C

FEE SCHEDULE

The Fee Schedule shall set forth all recurring fees, one-time fees, professional services rates, expense reimbursement rates, and any volume discounts or fee escalation mechanisms applicable to the Services.

EXHIBIT D

IT SECURITY ADDENDUM

[See attached IT Security Addendum]

EXHIBIT E

DATA PROCESSING AGREEMENT

The Data Processing Agreement governs Vendor's processing of Personal Data on behalf of Client and sets forth GDPR/CCPA-compliant controller-processor obligations, data subject rights procedures, subprocessor requirements, and cross-border transfer mechanisms.

EXHIBIT F

APPROVED SUBCONTRACTORS AND SUBPROCESSORS

The following Subcontractors and Subprocessors are approved as of the Effective Date: [List Name / Service / Location / Data Access Scope for each]. Changes require 30 days' prior written notice and Client's approval per Section 14.1.