THREATMODELER CLOUD SUBSCRIPTION AGREEMENT

(NA)

Last Updated: July 2026

APPLICABILITY: This North America (NA) version of the Agreement applies solely to Customers established or domiciled in North America (including the United States and Canada) or where the contracting ThreatModeler entity is ThreatModeler Software, Inc.

This ThreatModeler Cloud Subscription Agreement (this "Agreement") governs the access to and use of ThreatModeler's cloud-based threat modeling platform and related services (the "Product"). This Agreement entered into by and between ThreatModeler Software, Inc., a Delaware corporation with its principal place of business at 101 Hudson Street, 21st Floor Jersey City, New Jersey 07302, USA ("ThreatModeler"); and the entity or individual identified as the customer in an applicable Order Form or that otherwise downloads, installs, or uses the Software ("Customer"). This Agreement takes effect on the date of the initial Order Form, or the date on which Customer first downloads or accesses the Software, whichever is earlier (the "Effective Date").

BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, BY CLICKING "I AGREE," OR BY ACCESSING OR USING THE PRODUCT, CUSTOMER AGREES TO BE BOUND BY THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT.

1. DEFINITIONS

1.1. "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where "control" means direct or indirect ownership of more than fifty percent (50%) of the voting interests of the subject entity.Notwithstanding the foregoing, an "Affiliate" shall not include any entity that is a direct competitor of ThreatModeler. ThreatModeler reserves the right, in its reasonable business judgment, to determine whether an entity qualifies as a direct competitor.

1.2. "Core AI Functionality" means any features, models, or autonomous agents within the Product that utilize machine learning or artificial intelligence technologies to analyze, generate, or automate threat models, security requirements, and design content. The Core AI Functionality operates in: (a) "Default AI Mode," where ThreatModeler processes data using its designated third-party AI subprocessors, or (b) "BYOAI Mode," where Customer configures the Product to process data using its own designated third-party AI provider.

1.3. "Authorized User" means a specific, uniquely identified individual (an employee or contractor of Customer or its Affiliates) who has been authorized by Customer to access and use the Product. Each Authorized User must be assigned unique user credentials (e.g., a unique user ID and password), and a user license may not be shared or used by more than one individual. However, user licenses may be permanently reassigned to a new individual replacing one who has terminated their employment or contract, or otherwise changed job status or function and no longer requires access to the Product. Customer is fully responsible for all acts and omissions of its Authorized Users.

1.4. "Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, 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. "Confidential Information" includes, without limitation: (a) For ThreatModeler: The Product and Services in their entirety, including their underlying technology, source code, AI prompts, rules, agent workflows, telemetry, performance data, security reports, product roadmaps, and pricing; (b) For Customer: The Customer Data (Inputs), and any Customer-specific system vulnerabilities, security gaps, or proprietary architectural details contained within any generated Outputs; (c) For Both Parties: The terms and conditions of this Agreement and all Order Forms. Confidential Information does not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation; (iii) is received from a third party without breach of any obligation; or (iv) was independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

1.5. "Customer Data" means any proprietary information, data, or materials uploaded, submitted, or inputted into the Product by Customer or its Authorized Users ("Inputs"). For the avoidance of doubt, Customer Data does not include any threat libraries, security controls, templates, rules, or threat modeling intelligence pre-existing within or generated by the Product ("ThreatModeler Content").
1.6. "Documentation" means ThreatModeler's official, generally available technical and functional documentation for the applicable Product, as made available on ThreatModeler's support portal or other designated website. For the avoidance of doubt, "Documentation" specifically excludes any and all marketing materials, websites, press releases, proposals, or non-technical blog posts, and shall not be construed as a warranty or commitment for the development or delivery of any future functionality or features.
1.7. "Feedback" means any suggestion, enhancement request, recommendation, correction, or other feedback provided by Customer or its Authorized Users relating to the operation or functionality of the Product.
1.8. "Intellectual Property Rights" means any and all registered and unregistered rights granted, applied for, or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection, or other intellectual property law, and all similar or equivalent rights or forms of protection, in any part of the world. This includes, without limitation:(a) all rights in and to inventions (whether patentable or not), discoveries, and improvements; (b) all rights in and to works of authorship, including copyrights, mask work rights, and moral rights; (c) all rights in and to trade names, logos, trademarks, and service marks (together with all of the goodwill associated therewith); (d) all rights in and to confidential information, know-how, and trade secrets; and (e) all rights in and to domain names, website designs, and user interface designs.
1.9. "Order" means the binding transactional document for the purchase of Products. An Order is formed when: (a) Customer executes a "Quote" or "Order Form" issued by ThreatModeler; or (b) ThreatModeler accepts, in writing or by beginning performance, a "Purchase Order" or "PO" issued by Customer against a valid Quote. A PO issued by Customer becomes a binding Order only upon ThreatModeler's written acceptance. For the avoidance of doubt, any Purchase Order issued by Customer is accepted by ThreatModeler solely for the purpose of administrative convenience, invoicing, and billing; any pre-printed, standard, or conflicting terms and conditions contained in or attached to such Customer-issued PO are hereby expressly rejected by ThreatModeler and shall be null, void, and of no legal force or effect, as set forth in Section 14.13(c).
1.10. "Product(s)" means the commercially available offerings of ThreatModeler subscribed to by Customer as identified in an applicable Order. Unless otherwise specified in an Order, the core "Product" subscription consists of the following components: (a) A subscription to access and use the "Platform," which refers to ThreatModeler's proprietary cloud-based software, including its integrated "Core AI Functionality"; (b) Any "Updates" to the Platform that ThreatModeler makes generally available to its subscribed customers; (c) The applicable tier of "Support Services," as set forth in Section 1.14; (d) Access to the official "Documentation." For the avoidance of doubt, Professional Services and Training are not included as part of the standard Product subscription and must be purchased separately pursuant to an Order and governed by a Statement of Work (SOW). The term "Product" explicitly excludes any third-party software, hardware, or services required by Customer to access or use the offering.
1.11. "Professional Services" means expert services provided by ThreatModeler to Customer, which are separate from the subscribed Product and are governed by a Statement of Work ("SOW"). Professional Services are purchased on a project or time-and-materials basis and may include, but are not limited to, implementation assistance, system configuration, dedicated training, and custom content or report creation. Unless otherwise expressly agreed in a SOW, all Professional Services are provided on a non-"work-for-hire" basis. All intellectual property rights in any deliverables, tools, or methodologies used or created by ThreatModeler in the course of providing Professional Services shall remain the exclusive property of ThreatModeler, subject to the limited license rights granted to Customer in the applicable SOW or Section 13.4 of this Agreement. The successful delivery of Professional Services is dependent on Customer's timely cooperation and fulfillment of its responsibilities as outlined in the applicable SOW.
1.12."Scope of Use" means the specific usage limits, tiers, and metrics for the purchased Product subscription, as expressly set forth in the applicable Order. Common metrics include, but are not limited to, the number of Authorized Users and the number of Threat Models. Customer's use of the Product must not exceed the Scope of Use.
1.13. "Subscription Term" means the initial term for the subscription to the Services as specified in an Order, and any subsequent renewal terms.
1.14."Support Services" means the technical support, maintenance, and service level commitments provided by ThreatModeler for the subscribed Product. The specific scope, support channels, response times, and uptime commitments for the Support Services are detailed in the ThreatModeler Support Services Policy and Service Level Agreement ("SLA") available at threatmodeler.ai/legal/support-program.

2. LICENSE, SUPPORT, AND UPDATES

2.1. Subscription and Access Rights. Subject to Customer's full and timely payment of all applicable fees and its continuous compliance with the terms of this Agreement, ThreatModeler grants Customer a subscription for its Authorized Users to access and use the subscribed Product during the applicable Subscription Term. This subscription includes a limited, non-exclusive, non-transferable, and non-sublicensable right to access and use the Product, solely for Customer's internal business purposes

and strictly within the Scope of Use defined in the applicable Order. Customer agrees that no user license will be provided to any employee or contractor of an Affiliate that is a direct competitor of ThreatModeler, as determined in accordance with Section 1.1.

2.2. Support, Maintenance, and Updates. ThreatModeler will provide technical support and maintenance for the Product in accordance with the Support Services Policy and SLA referenced in Section 1.14. ThreatModeler reserves the right to update the Support Services Policy from time to time, provided that any such update will not result in a material and adverse decrease of the Support Services or SLA commitments during Customer's then-current Subscription Term.

2.3. Product Modifications. Customer acknowledges that the Product is an evolving, subscription-based offering. ThreatModeler reserves the right to enhance or modify the Product from time to time. However, ThreatModeler will not, during an active Subscription Term, make any changes that result in a material diminution of the overall functionality and value of the Product as it existed at the beginning of that Term.

3. ACCEPTABLE USE AND CUSTOMER OBLIGATIONS

3.1. General Responsibilities. Customer is and shall remain solely responsible and liable for:
(a) Authorized User Conduct: All activities conducted by its Authorized Users within the Product, and for ensuring their compliance with the terms of these . A breach by an Authorized User is deemed a breach by Customer.
(b) Customer Data: The accuracy, legality, quality, and integrity of all Customer Data, including obtaining all necessary rights, consents, and permissions to provide, use, and process the Customer Data as contemplated by this Agreement.
(c) Account Security: Maintaining the security and confidentiality of all Authorized User account credentials and for promptly notifying ThreatModeler of any unauthorized access or use.
(d) Compliance with Laws: Ensuring that its use of the Product complies with all applicable local, state, federal, and international laws and regulations.

3.2. Use Restrictions. Customer shall not, and shall not permit any Authorized User or any third party to, perform any of the following actions:
(a) Resale and Sublicensing: Sell, resell, lease, sublicense, or otherwise provide access to the Product to any third party, or use the Product to provide service bureau, timesharing, or other managed services for the benefit of any third party.
(b) Modification and Derivative Works: Modify, translate, adapt, or create derivative works based upon the Product or any part thereof.
(c) Reverse Engineering: Reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code, underlying ideas, or non-public APIs of the Product, except to the extent such a restriction is expressly prohibited by applicable law.
(d) Interference: Interfere with, disrupt, or create an undue burden on the integrity, performance, or security of the Product or the data contained therein.
(e) Security Testing: Conduct any security assessments, penetration tests, vulnerability scans, or load testing on the Product or its infrastructure without the prior express written consent and coordination of ThreatModeler.
(f) Malicious Use: Use the Product to store or transmit any viruses, worms, Trojan horses, or other malicious code, or to engage in any phishing, spamming, or denial-of-service attacks.
(g) Unlawful or Infringing Content: Use the Product to store or transmit any content that is infringing, libelous, or otherwise unlawful or tortious, or that violates the privacy or intellectual property rights of any third party.
(h) Public Benchmarking: Publicly disseminate any performance information, analysis, or competitive

benchmarks of the Product without ThreatModeler's prior written consent.
(i) Circumvention: Attempt to circumvent any Scope of Use restrictions or other license control mechanisms within the Product.
(j) Multiplexing and Pooling: Use any technology, software, script, or automated agent to pool connections, redirect requests, or "multiplex" access to the Product in a manner that bypasses the Authorized User license limits, or allows unlicensed individuals to indirectly access, query, or utilize the Product's functionalities.

3.3. High-Risk Activities Prohibition. The Product is not designed, manufactured, or intended for use in hazardous environments requiring fail-safe performance, including but not limited to the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems ("High-Risk Activities"). Customer expressly agrees that it will not use, or permit the use of, the Product for any High-Risk Activities. ThreatModeler and its suppliers expressly disclaim any express or implied warranty of fitness for such purposes.

3.4. Prohibition on Sensitive Personal Information. Customer agrees that it shall not upload or process any "Sensitive Data" in the Product. Customer acknowledges that the Product is not designed for such data and ThreatModeler has no liability for any Sensitive Data processed in violation of this section.

"Sensitive Data" includes any data that requires heightened protection under applicable law, including, but not limited to, health information (HIPAA), financial information (GLBA, PCI DSS), government-issued IDs, and "special categories of personal data" under GDPR.

Customer shall indemnify, defend, and hold harmless ThreatModeler from any damages, losses, and costs arising from or related to Customer's breach of this Section 3.4.

4. FEES, PAYMENT, AND AUDITS

4.1. Fees. Customer shall pay all fees specified in all applicable Orders ("Fees"). Except as expressly provided in this Agreement, all payment obligations are non-cancellable and all Fees paid are non-refundable. The Fees are based on the Product subscription purchased and not on actual usage.

4.2. Invoicing and Payment. Unless otherwise specified in an Order Form, all Fees will be invoiced annually in advance. All invoices are due and payable net thirty (30) days from the invoice date, without offset or deduction. Late payments will accrue interest at a rate of 1.5% per month or the maximum rate permitted by law, whichever is lower.

4.3. Taxes.
a) Fees are stated exclusive of any taxes, levies, duties, or similar governmental assessments, including value-added, sales, use, or withholding taxes (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder.
b) If ThreatModeler has the legal obligation to pay or collect Taxes for which Customer is responsible, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides ThreatModeler with a valid tax exemption certificate.
c) If Customer is required by law to withhold any Taxes from its payments to ThreatModeler, Customer must provide ThreatModeler with an official tax receipt or other appropriate documentation. Customer agrees to increase the payment to ThreatModeler by the amount necessary to ensure that ThreatModeler receives a net amount equal to the full amount of the Fees it would have received without the deduction.

4.4. Suspension of Service and Termination. If any invoiced amount is more than thirty (30) days overdue, ThreatModeler may, without limiting its other rights and remedies: (a) suspend Customer's access to the Product upon ten (10) days' written notice until such amounts are paid in full, and (b) if the

failure to pay continues for sixty (60) days or more, terminate this Agreement for cause under Section 5.3.

4.5. Invoice Disputes. Customer must notify ThreatModeler in writing of any good-faith dispute with respect to an invoice within fifteen (15) days of the invoice date. If Customer fails to do so, Customer is deemed to have waived its right to dispute that invoice, and the invoice will be considered final and payable.

4.6. Usage Verification. Customer acknowledges and agrees that the Product includes a self-auditing function that electronically monitors and reports on Customer's usage metrics (e.g., number of Authorized Users, number of Threat Models). ThreatModeler shall have the right to use this reporting data to verify Customer's compliance with the Scope of Use.

If Customer's use of the Product exceeds its purchased entitlement as set forth in the applicable Order, ThreatModeler will invoice Customer for such overage at ThreatModeler's then-current list prices for the entire period of non-compliance. Customer agrees to pay such invoice in accordance with Section 4.2 of this Agreement.

5. TERM AND TERMINATION

5.1. Agreement Term. The term of this Agreement commences on the Effective Date and continues as long as a Subscription Term for any Product is in effect, unless terminated earlier in accordance with its terms.

5.2. Subscription Term and Auto-Renewal. Each Subscription Term will automatically renew for additional periods equal to the expiring term (or one year, if the expiring term is longer than one year), unless either party gives the other written notice of non-renewal at least sixty (60) days before the end of the then-current Subscription Term. ThreatModeler reserves the right to increase the fees for any renewal term by providing notice thereof at least fifteen (15) days prior to the end of the current term.

5.3. Termination for Cause. A party may terminate this Agreement for cause: (i) upon thirty (30) days' written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, or assignment for the benefit of creditors.

5.4. Termination for Convenience by Customer. Customer may terminate this Agreement for its convenience at any time by providing ninety (90) days' prior written notice to ThreatModeler. Upon such termination, Customer shall not be entitled to any refund, credit, or pro-rata return of any Fees paid upfront (as all payment obligations are non-cancellable and all Fees paid are non-refundable under Section 4.1). Any unpaid Fees associated with the remaining duration of the committed Subscription Term shall become immediately due and payable.

5.5. Effect of Termination. Upon any termination or expiration of this Agreement: (a) all rights and subscriptions granted to Customer hereunder shall immediately terminate and Customer shall cease all use of the Product; (b) Customer shall immediately pay any unpaid fees accrued prior to the effective date of termination, as well as any future fees that become due under Section 5.4; and (c) each party will, upon request, promptly return or securely destroy all Confidential Information of the other party.

5.6. Data Portability and Deletion. Upon Customer's written request made within thirty (30) days after the effective date of termination, ThreatModeler will make Customer Data available for export. After this

30-day period, ThreatModeler will have no further obligation to maintain any Customer Data and will thereafter delete it in accordance with its standard policies.

5.7. Survival. The following sections shall survive any termination or expiration of this Agreement: Section 1 (Definitions), 4 (Fees, Payment, and Audits), 5.5 (Effect of Termination), 5.7 (Survival), 6 (Confidentiality), 7 (Intellectual Property Rights), 9 (Mutual Indemnification), 10 (Limitation of Liability), and 14 (General Provisions).

5.8. Reinstatement of Lapsed Subscription. If any subscription for a Product expires or is terminated, and Customer seeks to reinstate such subscription at a later date, such reinstatement shall be subject to ThreatModeler's then-current policies. At a minimum, reinstatement will require Customer to pay: (a) a reinstatement fee; (b) all subscription fees that would have been payable during the period of the lapse; and (c) the subscription fees for the new Subscription Term.

6. DATA PROTECTION AND SECURITY

6.1. Security Program and Safeguards. ThreatModeler will implement and maintain a comprehensive written information security program, which includes administrative, physical, and technical safeguards aligned with accepted industry standards. This program is designed to protect the security, confidentiality, and integrity of Customer Data against accidental or unlawful destruction, loss, alteration, or unauthorized access, use, or disclosure. ThreatModeler will not materially decrease the overall security of the Product during a Subscription Term.

6.2. Data Processing, DPA, and Subprocessors.

(a) Data Processing Addendum. The parties acknowledge and agree that with respect to the processing of "Personal Data", ThreatModeler acts as a "Processor" or "Service Provider" and Customer is the "Controller" or "Business". All processing of Personal Data is subject to and governed by ThreatModeler's Data Processing Addendum ("DPA"), located at threatmodeler.ai/legal/dpa, which is hereby incorporated by reference.

(b) Subprocessors. Customer acknowledges that ThreatModeler uses third-party subprocessors to provide the Product. A current list of ThreatModeler's subprocessors is maintained at threatmodeler.ai/legal/subprocessors (the "Subprocessor List").

(c) New Subprocessors and Right to Object. ThreatModeler will provide Customer with at least fifteen (15) days' prior written notice of any new subprocessor appointment by updating the Subprocessor List and notifying Customer of such update. Customer may, within fifteen (15) days of such notice, object in writing to the new subprocessor on reasonable, data protection-related grounds. If the parties cannot resolve the objection, Customer may, as its sole and exclusive remedy, terminate the applicable subscription for cause.

6.3. Security Incident Response.

(a) Notification. ThreatModeler will notify Customer without undue delay upon becoming aware of a "Security Incident," which is defined as the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Customer Data processed by ThreatModeler.

(b) Cooperation. ThreatModeler will provide reasonable cooperation to Customer in the investigation of the Security Incident, including providing any relevant information reasonably requested by Customer regarding the nature of the incident, the categories of data affected, and the corrective actions being taken.

6.4. Customer's Security Responsibilities. Customer acknowledges that its security responsibilities are a critical component of overall data protection. Customer is solely responsible for: (a) securely managing all Authorized User account credentials; (b) configuring and using the Product in a secure manner in accordance with the Documentation; and (c) ensuring the security of its own systems and devices used to

access the Product and (d) notifying ThreatModeler of any known or suspected security breach originating from its own systems or involving its Authorized User account credentials.

7. CONFIDENTIALITY

7.1. Obligation of Confidentiality. The Receiving Party shall:
(a) use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than a reasonable degree of care);
(b) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement; and
(c) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information to those of its and its Affiliates' employees, contractors, and agents who have a legitimate "need to know" for purposes consistent with this Agreement and who are bound by confidentiality obligations containing protections no less stringent than those herein. The Receiving Party shall be liable for any breach of this Section 7 by its representatives.

7.2. Compelled Disclosure. A Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law or a valid court order to do so, provided the Receiving Party gives the Disclosing Party prior written notice of the compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest or seek a protective order for the disclosure.

7.3. Injunctive Relief. The parties agree that a breach of this Section 7 may cause irreparable harm for which monetary damages would not be an adequate remedy. Accordingly, the Disclosing Party shall be entitled to seek injunctive or other equitable relief to prevent or curtail any such breach, without the necessity of posting a bond.

8. INTELLECTUAL PROPERTY RIGHTS

8.1. ThreatModeler's Intellectual Property.
As between the Parties, ThreatModeler and its licensors exclusively own and retain all right, title, and interest in and to the Product, including the Platform, all generated threat models, reports, security requirements, and outputs (collectively, "Outputs"), and all underlying software, threat libraries, and technology.

Subject to Customer's payment of all Fees, ThreatModeler hereby grants Customer a non-exclusive, non-transferable, non-sublicensable license to use, copy, and distribute the Outputs solely for Customer's internal business and compliance purposes during the applicable Subscription Term, provided that Customer shall retain all rights in its proprietary Inputs contained within such Outputs.

8.2. Customer's Intellectual Property.
As between the parties, Customer exclusively owns and retains all right, title, and interest in and to the Customer Data, including all intellectual property rights therein.

8.3. License from Customer to Provide the Product.
Customer hereby grants ThreatModeler and its Affiliates a worldwide, limited-term, non-exclusive, royalty-free license to host, copy, transmit, process, and display Customer Data as reasonably necessary for ThreatModeler to provide, maintain, and support the Product for Customer in accordance with this Agreement. This license terminates upon the deletion of Customer Data as described in Section 5.6.

8.4. Ownership of Feedback.
Customer acknowledges and agrees that any suggestions, enhancement requests, recommendations, corrections, or other feedback provided by Customer or its Authorized Users relating to the operation of the Product ("Feedback") shall be owned by ThreatModeler. Customer hereby assigns to ThreatModeler

all right, title, and interest in and to any Feedback, without any right to compensation. ThreatModeler is under no obligation to use or implement any Feedback.

8.5. ThreatModeler's Rights to Use Non-Identifiable Data.

(a) Data Collection and Ownership. Customer acknowledges and agrees that ThreatModeler has the right to collect, analyze, and use technical, operational, and telemetry data relating to the provision, use, and performance of the Product, including data derived from Customer Data (collectively, "Usage Data"). For the avoidance of doubt, ThreatModeler shall exclusively own all right, title, and interest in and to the Usage Data.

(b) Permitted Uses. Provided that such Usage Data is in an aggregated and de-identified format that does not, and cannot be used to, identify Customer, its Affiliates, or any individual ("Anonymized Data"), ThreatModeler shall have the perpetual, irrevocable, worldwide, royalty-free right to use, reproduce, modify, and create derivative works of such Anonymized Data for any lawful business purpose.

(c) Illustrative Examples of Permitted Uses. Without limiting the generality of the foregoing, these business purposes include, but are not limited to:
i. Product Improvement: Analyzing usage patterns to enhance and optimize the Product's performance, security, and usability.
ii. New Feature Development: Using insights from Anonymized Data to inform the development of new features, products, and services.
iii. Benchmarking and Industry Analysis: Creating and publishing aggregated statistical reports, industry trend analyses, and benchmarks (e.g., "average number of threats identified in the financial services sector").

(d) Clarification on Customer Data. For the absolute avoidance of doubt, ThreatModeler will not use Customer's un-anonymized, identifiable Customer Data for any purpose other than providing the Product to Customer as described in this Agreement.

8.6. API and Integration Intellectual Property.
To the extent that Customer develops any custom connectors, scripts, or software integrations designed to connect Customer's internal tools or IDEs to the Product via ThreatModeler's Application Programming Interfaces (APIs) or the Model Context Protocol (MCP) Server (collectively, "Integrations"), Customer shall retain ownership of its custom code for such Integrations.
However, Customer acknowledges and agrees that: (a) such Integrations shall not be construed as creating any joint intellectual property rights, (b) ThreatModeler retains exclusive ownership of the underlying APIs, the MCP Server technology, and the platform architecture, and (c) nothing in this Agreement shall restrict ThreatModeler from independently developing, licensing, or commercializing similar integrations, connectors, or features for its other customers.

9. WARRANTIES AND DISCLAIMERS

9.1. Mutual Warranties. Each party represents and warrants that it has the legal power and authority to enter into this Agreement and that it will comply with all applicable laws in its performance hereunder.

9.2. Limited Performance Warranty. ThreatModeler warrants that, during an applicable Subscription Term, the Product will perform materially in accordance with the applicable Documentation. For any breach of this warranty, Customer's sole and exclusive remedy shall be the Service Credits as specified in the Support Services Policy located at threatmodeler.ai/legal/support-program.

9.3. WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS WARRANTIES PROVIDED IN SECTION 9.2 AND SECTION 13 OF THIS AGREEMENT, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT AND ANY SERVICES ARE PROVIDED "AS IS". WHILE

THREATMODELER WARRANTS IT WILL USE COMMERCIALLY REASONABLE SKILL AND CARE IN PROVIDING THE PRODUCT, IT EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. CUSTOMER ACKNOWLEDGES THAT ANY OUTPUTS, SUGGESTIONS, OR CONTENT GENERATED BY THE CORE AI FUNCTIONALITY ARE PROVIDED FOR INFORMATIONAL PURPOSES ONLY, WITHOUT WARRANTY OF ANY KIND, AND CUSTOMER IS SOLELY RESPONSIBLE FOR REVIEWING, VALIDATING, AND TESTING THE ACCURACY AND APPROPRIATENESS OF ANY SUCH OUTPUTS. THREATMODELER DOES NOT WARRANT THAT THE USE OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE. CUSTOMER ACKNOWLEDGES AND AGREES THAT THREATMODELER SHALL NOT BE LIABLE FOR DELAYS, INTERRUPTIONS, SERVICE FAILURES, OR OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS OR OTHER SYSTEMS OUTSIDE THE REASONABLE CONTROL OF THREATMODELER.

10. INDEMNIFICATION

10.1. Indemnification by ThreatModeler. ThreatModeler will defend Customer against any third-party claim, demand, suit, or proceeding ("Claim") alleging that Customer's use of the Product, as delivered by ThreatModeler and used in accordance with this Agreement, directly infringes a valid U.S. patent, copyright, or registered trademark of such third party. ThreatModeler will indemnify Customer for any damages, attorney fees, and costs finally awarded against Customer as a result of, or for amounts paid by Customer under a court-approved settlement of, such a Claim.

10.2. Mitigation and Remedy. If the Product becomes, or in ThreatModeler's opinion is likely to become, the subject of an infringement Claim, ThreatModeler may, at its option and expense:
(a) procure for Customer the right to continue using the Product;
(b) replace or modify the Product with a non-infringing but functionally equivalent alternative; or
(c) if options (a) and (b) are not commercially reasonable, terminate Customer's subscription for the infringing Product and provide a pro-rata refund of any prepaid fees for the remainder of the terminated Subscription Term.

10.3. Exclusions. ThreatModeler's obligations under Section 10.1 will not apply to any Claim to the extent it arises from: (a) use of the Product in combination with hardware, software, or data not provided by ThreatModeler; (b) Customer Data; (c) any modification to the Product not made by ThreatModeler; or (d) Customer's use of a version of the Product other than the then-current version, if the infringement would have been avoided by use of the current version made available to Customer.

10.4. Indemnification by Customer. Customer will defend ThreatModeler against any Claim made or brought against ThreatModeler by a third party arising from or related to: (i) the Customer Data, including any allegation that the Customer Data infringes or misappropriates the rights of a third party; or (ii) Customer's use of the Product in breach of this Agreement or applicable law. Customer will indemnify ThreatModeler for any damages, attorney fees, and costs finally awarded against ThreatModeler as a result of, or for amounts paid by ThreatModeler under a court-approved settlement of, such a Claim.

10.5. Indemnification Procedure. The indemnifying party's obligations are contingent upon the indemnified party: (a) promptly giving written notice of the Claim; (b) giving the indemnifying party sole control of the defense and settlement of the Claim (provided that the indemnifying party may not settle any Claim unless the settlement unconditionally releases the indemnified party of all liability and does not include a statement as to, or an admission of, fault, culpability, or failure to act by or on behalf of the indemnified party); and (c) providing all reasonable assistance, at the indemnifying party's expense.

10.6. Exclusive Remedy. This Section 9 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of third-party infringement claim described in this section.

11. LIMITATION OF LIABILITY

11.1. DISCLAIMER OF INDIRECT AND CONSEQUENTIAL DAMAGES.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY OR ITS SUPPLIERS HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS, LOST DATA, LOSS OF USE, BUSINESS INTERRUPTION, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

11.2. LIMITATION OF AGGREGATE LIABILITY.
TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE TOTAL AMOUNT OF FEES ACTUALLY PAID BY CUSTOMER TO THREATMODELER HEREUNDER IN THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE FIRST INCIDENT GIVING RISE TO THE LIABILITY.

11.3. EXCLUSIONS FROM LIMITATIONS ("UNLIMITED LIABILITY CARVE-OUTS").
THE LIMITATIONS SET FORTH IN SECTIONS 11.1 AND 11.2 SHALL NOT APPLY TO:
(a) A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 10;
(b) A VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS;
(c) CUSTOMER'S UNPAID PAYMENT OBLIGATIONS FOR FEES DUE UNDER ANY ORDER FORM; OR
(d) LIABILITY ARISING FROM A PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

11.4. Allocation of Risk. The parties acknowledge and agree that the essential purpose of this Section 11 is to allocate the risks under this Agreement between the parties and that the fees have been set and this Agreement entered into in reliance upon these limitations of liability.

12. CORE AI FUNCTIONALITY
12.1. General and Disclaimer of Warranties. The Product includes Core AI Functionality designed to enhance the threat modeling process. Customer retains full control over the use of this functionality and is solely responsible for reviewing, validating, and accepting any output generated by it. CUSTOMER ACKNOWLEDGES AND AGREES THAT AI-GENERATED OUTPUTS ARE SUBJECT TO MACHINE LEARNING LIMITATIONS AND MAY OCCASIONALLY CONTAIN ERRORS, OMISSIONS, OR INCORRECT THREAT PREDICTIONS ("HALLUCINATIONS"). ALL AI-GENERATED OUTPUT IS PROVIDED STRICTLY "AS IS," WITHOUT WARRANTY OF ANY KIND, AND ITS USE IS AT CUSTOMER'S SOLE RISK AND DISCRETION.
12.2. Default AI Mode and Data Processing. Unless Customer configures the BYOAI Mode, the Product will operate in Default AI Mode, using ThreatModeler's designated AI subprocessor as listed on its Subprocessor List. In this mode, ThreatModeler will process Customer Data, including Inputs and Outputs, solely to provide the Core AI Functionality.
12.3. BYOAI Mode. If Customer subscribes to and configures the "Bring Your Own AI" (BYOAI) functionality, Customer may connect its own third-party AI provider account. In BYOAI Mode, Customer acknowledges that:
(a) All AI-related processing will occur directly between ThreatModeler and Customer's designated AI provider, under the terms of the agreement between Customer and that provider.

(b) Customer's AI provider is not a subprocessor of ThreatModeler. Customer is solely responsible for the security, privacy, and compliance of its relationship with its AI provider.

12.4. Optional AI Model Improvement Program.

(a) Participation. To improve the accuracy, relevance, and performance of ThreatModeler's proprietary AI models, Customer agrees that ThreatModeler may utilize Anonymized Data (as defined in Section 8.5(b)) derived from Customer's Inputs and Outputs to train, validate, and improve such models by default.

(b) Right to Opt-Out. Customer's participation in the AI model improvement program is entirely voluntary. Customer may, at any time during the Subscription Term, opt-out of this program by submitting a written request via email to privacy@threatmodeler.com.

(c) Effect of Opt-Out. Upon receipt of such opt-out request, ThreatModeler shall ensure that the Customer's tenant configuration is set to restrict any data extraction for AI training, and shall immediately cease using any new Anonymized Data derived from Customer's account for AI model training purposes.

(d) No Training Without Consent. For the avoidance of doubt, unless Customer participates in the default Anonymized Data program or provides explicit consent, ThreatModeler will never use any un-anonymized, identifiable Customer Data (Inputs) to train, fine-tune, or develop any general or publicly available artificial intelligence models.

13. PROFESSIONAL SERVICES

13.1. Scope and Governance. ThreatModeler will provide Customer with the Professional Services, if any, as described in one or more mutually executed Statements of Work ("SOWs"). Each SOW will detail the specific scope, deliverables, timelines, fees, and any other terms applicable to a particular project. Each SOW is hereby incorporated by reference into this Agreement. In the event of a direct conflict between the terms of a SOW and this Agreement, the terms of this Agreement shall prevail, unless the SOW expressly identifies the conflicting provision of this Agreement and states its intent to override it for that specific project.

13.2. Performance Warranty. ThreatModeler warrants that all Professional Services will be performed in a professional and workmanlike manner, in all material respects in accordance with the specifications set forth in the applicable SOW. For any breach of this warranty, Customer's sole and exclusive remedy shall be for ThreatModeler, at its option, to either: (a) re-perform the non-conforming Professional Services at no additional charge; or (b) if re-performance is not commercially feasible, terminate the applicable SOW and provide a pro-rata refund of the fees paid for the non-conforming portion of the Professional Services. To receive this remedy, Customer must report the non-conformity in writing within thirty (30) days of the completion of the services.

13.3. Customer Cooperation. Customer acknowledges that the successful and timely delivery of Professional Services requires its good-faith cooperation. Customer agrees to provide ThreatModeler with timely access to its personnel, facilities, and any necessary information or materials. ThreatModeler shall not be liable for any delay or failure in performance to the extent caused by Customer's failure to meet its responsibilities. Any delays caused by Customer may result in additional fees and adjustments to the project timeline.

13.4. Intellectual Property.

(a) ThreatModeler's Pre-Existing IP. ThreatModeler shall retain all right, title, and interest in and to any of its pre-existing tools, methodologies, know-how, and other intellectual property used or provided in the course of performing the Professional Services ("ThreatModeler Background IP").

(b) Deliverables. Upon Customer's payment in full of all applicable fees, any custom reports, configurations, or other deliverables created specifically for Customer as described in a SOW ("Deliverables") are licensed to Customer for its internal use only during its active Subscription Term for the related Product. ThreatModeler retains ownership of all intellectual property rights in and to the

Deliverables.
(c) No Work for Hire. For the avoidance of doubt, all Professional Services are provided on a non-"work-for-hire" basis.

13.5. Personnel and Expenses. ThreatModeler will determine the personnel assigned to perform the Professional Services. Unless otherwise specified in the applicable SOW, Customer will reimburse ThreatModeler for all reasonable, pre-approved travel and out-of-pocket expenses incurred in connection with the provision of Professional Services.

14. GENERAL PROVISIONS

14.1. Governing Law, Jurisdiction, and Venue. This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware, USA, without regard to its conflict of law principles. The parties irrevocably agree to the exclusive jurisdiction and venue of the state and federal courts located in the State of Delaware for the resolution of any dispute arising out of or relating to this Agreement. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this Agreement.

14.2. Notices. All notices under this Agreement shall be sent exclusively by email to legal@threatmodeler.com (for ThreatModeler) and to the primary email address associated with Customer's account or specified in the most recent Order Form (for Customer). Notices are deemed received upon successful transmission, provided no delivery failure is returned. Customer is solely responsible for keeping its email address current and operational.

14.3. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the parties.

14.4. No Third-Party Beneficiaries. This Agreement is for the sole benefit of the parties hereto and their respective successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other person or entity any legal or equitable right, benefit, or remedy of any nature whatsoever.

14.5. Subcontracting. ThreatModeler may use affiliates or other third-party contractors in the performance of its obligations hereunder, including for the provision of Support Services and Professional Services, provided that ThreatModeler shall remain fully responsible for the performance of any such subcontractor and for their compliance with all terms of this Agreement.

14.6. Assignment. Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld). Notwithstanding the foregoing, either party may assign this Agreement in its entirety, without the other party's consent, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets.

14.7. Force Majeure. Neither party shall be liable for any failure or delay in performance (except for payment obligations) due to a "Force Majeure Event," meaning causes beyond its reasonable control, including but not limited to acts of God, war, terrorism, riots, strikes, or natural disasters.

14.8. Export Compliance. The Product and related technology are subject to U.S. export control and economic sanctions laws. Customer is solely responsible for ensuring its compliance with all such laws. Customer represents and warrants that it is not located in any U.S. embargoed country and is not named on any U.S. government restricted or denied-party list. Customer shall not permit any Authorized User to access or use the Product in violation of any U.S. export law or regulation.

14.9. U.S. Government End Users. If Customer is an agency or instrumentality of the United States Government ("USG"), the Product and Documentation qualify as "commercial items" as defined at Federal Acquisition Regulation ("FAR") 48 C.F.R. 2.101. The use, duplication, and disclosure of the Product by the USG is subject to the restrictions set forth in this Agreement, consistent with FAR 12.212 and DFARS 227.7202. To the extent any provision of this Agreement conflicts with applicable federal law, such provision shall be deemed amended to be consistent with federal law.

14.10. Publicity. Neither party shall use the other party's name or logo in any press release, marketing materials, or other public announcement without the other party's prior written consent. However, ThreatModeler may identify Customer by name in its customer lists.

14.11. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of this Agreement will remain in effect.

14.12. Waiver. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right or any other right.

14.13. Entire Agreement, Order of Precedence, and Supremacy.
(a) Entire Agreement. This Agreement, including all Order Forms, SOWs, and Exhibits, constitutes the entire agreement between the Parties and supersedes all prior understandings, oral or written. Any amendment must be in writing and signed by both Parties.

(b) Order of Precedence. In the event of a conflict, the documents shall control in the following order: (1) this Agreement, (2) the SOW, (3) the Order Form. Notwithstanding the foregoing, a specific provision in an Order Form or SOW may supersede a conflicting provision in this Agreement only if it explicitly identifies the section number it intends to override (e.g., *"Notwithstanding Section 11.2 of the Agreement..."*) and is counter-signed by an authorized representative of ThreatModeler.

(c) Supremacy over Customer Forms. This Agreement and any ThreatModeler-issued Order Form shall prevail over any terms in a Customer-issued purchase order (PO), vendor portal, or other business form. All such Customer-provided terms are hereby rejected, null, and void. ThreatModeler's delivery of the Product or acceptance of payment shall not be construed as acceptance of Customer's terms, regardless of whether such Customer forms are signed by ThreatModeler.