ThreatMate Inc. Subscriber Terms of Use

Introduction

These Subscriber Terms of Use ("Terms") govern your access to and use of the ThreatMate Cybersecurity Platform and ThreatMate Services.

Please read the binding arbitration Section and class action waiver in Section 14.11. It affects how disputes are resolved.

By (1) clicking a box indicating acceptance of these Terms, (2) using the ThreatMate Cybersecurity Platform or any ThreatMate Services, or (3) consenting to an Order Form that references these Terms, You agree and become a party to these Terms. If the individual accepting these Terms is accepting on behalf of a company or other legal entity (each, a "Company Subscriber"), such individual represents that they have the authority to bind the Company Subscriber identified in the registration process (and its affiliates) to these Terms, in which case the term "you" refers to the Company Subscriber and its affiliates. If the individual accepting these Terms does not have such authority, or does not agree with these Terms, such individual must not accept these Terms and may not access or use the ThreatMate Cybersecurity Platform or any ThreatMate Services.

ThreatMate's direct competitors are prohibited from accessing or using the ThreatMate Cybersecurity Platform, except with ThreatMate's prior written consent. In addition, the ThreatMate Cybersecurity Platform may not be accessed for purposes of monitoring availability, performance or functionality, or for any other benchmarking or competitive purposes except with ThreatMate's prior written consent..

These Terms include the introduction above, plus; (a) the General Terms and Conditions in Exhibit A below; (b) the Definitions in Exhibit B below; (c) the then-current Website Terms of Use; (c) the Data Protection Addendum, as applicable, available to you via the ThreatMate Cybersecurity Platform; (d) any and all Order Forms; (e) any applicable Additional Terms; and (f) information contained in a URL or policy referenced in any of the foregoing. These Terms were last updated on November 6, 2023.

Exhibit A –General Terms And Conditions

1. **Definitions.** Terms defined either in Exhibit B, or in the context in which they first appear in these Terms (including any Order Form), will have the indicated meaning throughout

these Terms and all attached documents. Unless otherwise indicated, all Section references in these Terms are to sections in these General Terms and Conditions.

2. **Provision of ThreatMate Services.** Until expiration or termination of your Subscription Term, ThreatMate grants you a limited, revocable, worldwide, non-exclusive, non-transferable, non-assignable (except as expressly stated herein) license during the Subscription Term for you to access and use (if you are an individual subscriber) or for you to allow your Users to access and use (if you are a Company Subscriber) those functionalities of the ThreatMate Cybersecurity Platform and ThreatMate Services which are consistent with your Subscription Level, solely for your internal business purposes. Your right to access and use the ThreatMate Cybersecurity Platform and ThreatMate Services is (a) subject to your Subscription Level and your compliance with these Terms, including your timely payment of all applicable Fees, (b) not contingent on the delivery of any future functionality or features, and (c) not dependent on any oral or written comments made by ThreatMate regarding future functionality or features.

3. **Use of ThreatMate Cybersecurity Platform.**

3.1. **Your Responsibilities.** You will (a) be responsible for your (and for Company Subscribers, each User's) compliance with these Terms, (b) be solely responsible for the accuracy, quality, integrity, and legality of your Content and Applications, the means by which you and/or your Users acquired your Content or Applications, and you and your Users' rights to use your Content or Applications (c) use commercially reasonable efforts to prevent unauthorized access to or use of any ThreatMate Cybersecurity Platform account, and notify ThreatMate promptly of any such unauthorized access or use, (d) access and use, and cause your Users (if applicable) to access and use, the ThreatMate Cybersecurity Platform only in accordance with these Terms and applicable laws and government regulations, including those related to privacy, electronic communications, and anti-spam.

3.2. **No Modifications.** Neither you nor your Users may in any way: (a) modify, change, alter, or create derivatives works based upon the ThreatMate Cybersecurity Platform or ThreatMate Services; or (b) use the ThreatMate Cybersecurity Platform or any ThreatMate Services for any purpose that (i) violates applicable law or regulation or (ii) is not expressly authorized under these Terms.

3.3. **Usage Limits.** The ThreatMate Cybersecurity Platform and ThreatMate Services may be subject to usage limits. If you or your Users exceed a contractual usage limit, ThreatMate may work with you to seek to reduce your usage so that it conforms to that limit. If, notwithstanding ThreatMate's efforts, you are unable or unwilling to abide by a usage limit, you will pay any invoice for excess usage in accordance with the "Fees and Payment" section below.

3.4. **Usage Restrictions.** You will not, and will not permit your Users to (a) make the ThreatMate Cybersecurity Platform or any ThreatMate Services, or any portion thereof, available to anyone other than your Users, or use the ThreatMate Cybersecurity Platform or ThreatMate Services for the benefit of anyone other than you, (b) sell, resell, license, sublicense, distribute, make available, rent, or lease the ThreatMate Cybersecurity Platform or any ThreatMate Services, or any portion thereof, (c) use the ThreatMate Cybersecurity Platform or any ThreatMate Services to disseminate, store, or transmit infringing, libelous, or otherwise unlawful or tortious material, or to disseminate, store, or transmit material in violation of third-party

intellectual property or privacy rights, (d) use the ThreatMate Cybersecurity Platform or any ThreatMate Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of the ThreatMate Cybersecurity Platform or any ThreatMate Services, (f) attempt to gain unauthorized access to the ThreatMate Cybersecurity Platform or its related systems or networks, (g) permit direct or indirect access to or use of the ThreatMate Cybersecurity Platform or any ThreatMate Services in a way that circumvents any provision of these Terms, or use the ThreatMate Cybersecurity Platform or any ThreatMate Services to access or use any of ThreatMate's intellectual property (except as expressly permitted under these Terms), (h) modify, copy, or create derivative works based on the ThreatMate Cybersecurity Platform or any ThreatMate Services or any part, feature, function, or dashboard thereof, (i) copy the ThreatMate Cybersecurity Platform or any ThreatMate Services or any portion thereof (except as ThreatMate may expressly permit Vendors to copy certain pitch templates), (j) frame or mirror any part of the ThreatMate Cybersecurity Platform or any ThreatMate Services other than framing on your own intranets for your own internal business purposes, (k) except to the extent permitted by applicable law, disassemble, reverse engineer, or decompile the ThreatMate Cybersecurity Platform or any ThreatMate Services or access to them, (l) build a competitive product or service, (m) build a product or service using similar ideas, features, functions or graphics of the ThreatMate Cybersecurity Platform or any ThreatMate Services, or (n) copy any ideas, features, functions or graphics of the ThreatMate Cybersecurity Platform or any ThreatMate Services (except as ThreatMate may expressly permit Vendors to copy certain pitch templates). Any use of the ThreatMate Cybersecurity Platform or any ThreatMate Services in breach of this Section may result in immediate suspension or termination of your account, in ThreatMate's sole discretion; ThreatMate may, in its sole discretion, use commercially reasonable efforts under the circumstances to provide you with notice and an opportunity to remedy such breach or threat prior to any such suspension or termination.

4. **Notices and messages.**

4.1. By entering into these Terms or using the ThreatMate Cybersecurity Platform, and by providing telephone numbers and email accounts of your Users, you expressly agree and affirmatively consent: (a) to receive communications (i) from us, (ii) from our independent contractors and (ii) from other Subscribers, where the applicable ThreatMate Cybersecurity Platform functionality permits or requires communications or where you have indicated your consent to be contacted by such parties, including via e-mail, text message, calls, and push notifications or other messaging tools and features within the ThreatMate Cybersecurity Platform; and (b) that texts, calls, or prerecorded messages may be generated by automatic telephone dialing systems. Communications from us and our Affiliates may include: operational communications concerning your account or the use of the ThreatMate Cybersecurity Platform or ThreatMate Services, updates concerning new and existing features or offerings on the ThreatMate Cybersecurity Platform or with respect to ThreatMate Services, communications concerning promotions run by us or our third-party partners, or news concerning industry developments. Standard text messaging charges applied by your cell phone carrier may apply to text messages that we send. All such charges are billed by and payable to your cell phone carrier. You understand that you do not have to agree to receive automated promotional calls/texts as a condition of purchasing any goods or services. **If you wish to opt out of promotional emails, you can unsubscribe from our promotional email list by following the unsubscribe options**

in the promotional email itself. If you wish to opt out of promotional calls or texts, you may reply "stop" from the mobile device receiving the messages. If you wish to opt out of all texts or calls from us (including operational or transactional texts or calls), you can text the word "stopall" from the mobile device receiving the messages. However, you acknowledge that opting out of receiving all texts may impact your use of the ThreatMate Cybersecurity Platform or related ThreatMate Services. If you choose to discontinue or terminate these Terms, or lose or plan to give up your telephone number(s) that are linked to your account or any User, you will send a text message with the word "STOPALL" to our sending number you wish to opt-out of before stopping use of the mobile number provided to ThreatMate, and you agree to timely update all contact information in your account. You represent and warrant that you own and control all contact information linked to your ThreatMate Cybersecurity Platform account, including the email accounts and the telephone number(s).

4.2. You agree to indemnify ThreatMate and its Affiliates for any privacy, tort or other claims relating to your voluntary provision of a telephone number or email account that is not owned by you and/or your failure to promptly notify ThreatMate of any changes in your contact information, including telephone number. You agree to indemnify, defend and hold ThreatMate and its Affiliates harmless from and against any and all such claims, losses, liability, costs and expenses (including reasonable attorneys' fees). ThreatMate will have the exclusive right to choose counsel, at your expense, to defend any such claims.

5. **Proprietary Rights**

5.1. **Reservation of Rights.** Subject to the limited rights expressly granted in these Terms, ThreatMate, its Affiliates, and its and their licensors reserve all rights, title, and interest in and to the ThreatMate Cybersecurity Platform and all ThreatMate Services (including all updates, customizations, and/or modifications thereto), and its and their trade and service marks, and the Aggregate Data (defined below), including in each case all related intellectual property rights. No rights are granted to you or your Users other than as expressly set forth herein.

5.2. **Your Marks.** You authorize ThreatMate to display your name and logo: (a) on the ThreatMate Cybersecurity Platform and in connection with ThreatMate Services, in connection with your use thereof; and (b) subject to your prior written approval, on its web site and marketing materials which are not a part of the ThreatMate Cybersecurity Platform or ThreatMate Services. ThreatMate will not alter approved marketing materials which include your trademark or other proprietary rights notice without your prior written consent. ThreatMate has no ownership interest in any of your trademarks.

5.3. **Ownership of your Content.** As between ThreatMate and you, you exclusively own all rights, title, and interest in and to your Content. To the extent you embed or post your Content on the ThreatMate Cybersecurity Platform, you hereby grant ThreatMate and its Affiliates a nonexclusive, perpetual, royalty-free, transferable, and fully sub-licensable right to host, copy, transmit, use, reproduce, adapt, translate, distribute, publish, and publicly display and perform your Content throughout the world in any media, now known or hereafter devised, on and through the ThreatMate Cybersecurity Platform. You agree that ThreatMate shall have the right to: (a) access and use your Content (i) to provide, maintain, and update your account; (ii) for the purpose of providing statistical insights and analysis related to your Users' use of the ThreatMate

Cybersecurity Platform; and (b) anonymize and aggregate your Content ("Aggregate Data") to prepare reports, studies, analyses, and other work product resulting from such Aggregate Data; under no other circumstances (except as may be required by law) shall ThreatMate distribute or otherwise make available to any third party any data that is identifiable as your Content. Subject to the limited rights expressly granted hereunder, ThreatMate acquires no right, title, or interest from you under these Terms in or to any of your Content.

5.4. **Feedback.** You and your Users grant ThreatMate and its Affiliates a non-exclusive, worldwide, perpetual, irrevocable, royalty-free, transferable, and assignable license to use and incorporate into the ThreatMate Cybersecurity Platform and any ThreatMate Services, any suggestions, enhancement requests, recommendations, corrections, or other feedback provided by you or Users relating to the ThreatMate Cybersecurity Platform, any ThreatMate content and any Services.

6. Term & Termination.

6.1 Term of Agreement. These Terms commence on the date you first accept them, and continue until all Subscription Terms have expired or have been terminated.

6.2 Renewal of Subscription Terms. Unless otherwise provided in an applicable Order Form, the term of each subscription shall (a) be for one year (the "Subscription Term") and (b) automatically renew for additional periods equal to the expiring Subscription Term or one year (whichever is shorter), unless either party gives the other notice (email is acceptable) of non-renewal at least 30 days before the end of the expiring Subscription Term. The pricing during any renewal term may increase, provided that ThreatMate provides you notice of different pricing at least 45 days prior to the applicable renewal Subscription Term.

6.3 Termination. Either party may terminate these Terms, including all applicable Order Forms, immediately and without further notice upon (a) a material breach by the other party of a material term or condition of these Terms, if such breach remains uncured within 30 days after the non-breaching party gives written notice of breach to the breaching party, (b) the institution by or against the other party of insolvency, receivership, or bankruptcy proceedings or any other proceedings for the settlement of the other party's debts, (c) the other party making an assignment for the benefit of creditors, or (d) the other party's dissolution or ceasing to do business. A material breach under this Section includes your failure to pay any applicable Fees when due. Additionally, ThreatMate may terminate these Terms, including all Order Forms, at any time, without liability, effective immediately, by providing written notice to you: (x) if necessitated by changes in applicable law or regulations, licensing from third parties, or technology; or (y) you independently develop, acquire, or make available any tool or service that is directly competitive with the ThreatMate Cybersecurity Platform or any ThreatMate Content or Service.

6.4 Effect of Termination or Expiration. Upon the termination of these Terms or the expiration and non-renewal of a Subscription Term, you will immediately cease and desist from accessing and using the ThreatMate Cybersecurity Platform (including any applicable ThreatMate Services). Termination or expiration of these Terms or an applicable Order Form shall not extinguish any of your or ThreatMate's obligations under these Terms or the applicable Order

Form that, by their nature, continue after the date of termination or expiration, including the obligation to pay any unpaid but due Fees and the confidentiality obligations of each party hereunder

7. Fees and Payment.

7.1 **Fees.** You will pay all fees applicable to your Subscription Level ("Fees"). Except as otherwise specified in an applicable Order Form: (a) Fees are based on subscriptions to the ThreatMate Cybersecurity Platform and ThreatMate Services, not actual usage; and (b) payment obligations are non-cancelable and Fees paid are non-refundable. Fees are fixed for one calendar year from the initial effective date of the first Subscription Term, but may be modified thereafter as set forth in Section 6.2.

7.2. **Invoicing and Payment.** You will provide ThreatMate with valid and updated credit card information, or with a valid purchase order or alternative payment method acceptable to ThreatMate. If you provide credit card information to ThreatMate, you authorize ThreatMate to charge such credit card for all Fees due hereunder. Except as otherwise set forth in an applicable Order Form, payment of Fees shall be made in advance, monthly or annually or in accordance with any different billing frequency stated in the applicable Order Form. Unless otherwise stated in an applicable Order Form, invoiced Fees are due upon execution of the order. You are responsible for providing complete and accurate billing and contact information to ThreatMate and notifying ThreatMate of any changes to such information, as well as for payment of any fees or charges associated with your payment other than those charged by ThreatMate's or its Affiliate's bank.

7.3 **Overdue Charges.** If payment of any Fees is not received by ThreatMate by the due date, without limiting ThreatMate's other rights or remedies: (a) unpaid Fees may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, and/or (b) ThreatMate may condition future subscription renewals and Order Forms on payment terms shorter than those specified in the "Invoicing and Payment" section above.

7.4 **Suspension and Acceleration.** If any Fees are 30 days or more overdue, (or ten or more days overdue in the case of amounts you have authorized ThreatMate to charge to your credit card), ThreatMate may, without limiting its other rights and remedies, accelerate your unpaid Fees obligations so that all such obligations become immediately due and payable, and/or suspend your access to the ThreatMate Cybersecurity Platform and ThreatMate Services until such amounts are paid in full; provided that if you are paying by credit card or direct debit and payment has been declined by the applicable financial institution, ThreatMate will give you at least ten days' prior notice that your payment is overdue before suspending your access to the ThreatMate Cybersecurity Platform.

7.5 **Payment Disputes.** ThreatMate will not exercise its rights under the "Overdue Charges" or "Suspension and Acceleration" sections above for 60 days if you are disputing the applicable Fees reasonably and in good faith and are cooperating diligently to resolve the dispute.

7.6 **Taxes.** Fees do not include any taxes, levies, duties, or similar governmental assessments of any nature, including value-added, sales, use, or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "Taxes"). You are responsible for paying all Taxes associated with purchases hereunder. If ThreatMate has the legal obligation to pay or collect Taxes for which you are responsible under this Section, ThreatMate will invoice you and you will pay that amount unless you provide ThreatMate with a valid tax exemption certificate authorized by the appropriate taxing authority. For clarity, ThreatMate is solely responsible for taxes assessable against it based on its income, property, and employees.

8. Confidentiality.

8.1 **Definition of Confidential Information.** "Confidential Information" means all non-public information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether electronically, 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/or the circumstances of disclosure. ThreatMate's Confidential Information includes the ThreatMate Cybersecurity Platform, ThreatMate Services, the Aggregate Data, contact and identity information of Subscribers and visitors to any ThreatMate website, and those other Subscribers provided to or accessible to you as part of the ThreatMate Cybersecurity Platform, and the terms and conditions of these Terms (including all Order Forms and pricing). Confidential Information of each party includes business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information does not include any information that: (a) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (b) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (c) is received from a third party without breach of any contractual, legal, or fiduciary obligation owed to the Disclosing Party; or (d) was independently developed by the Receiving Party without reference to, or reliance upon, the Confidential Information of the Disclosing Party. Each party retains all ownership, right, and title in and to its Confidential Information.

8.2. **Protection of Confidential Information.** Except as otherwise permitted in writing by the Disclosing Party, the Receiving Party will (a) use the same degree of care that it uses to protect the confidentiality of its own confidential information (but in no event less than reasonable care) to protect the Confidential Information of the Disclosing Party; (b) not use any Confidential Information of the Disclosing Party for any purpose not authorized by these Terms; and (c) except as otherwise authorized by the Disclosing Party in writing, limit access to, and disclosure of, the Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with these Terms and who have signed confidentiality agreements with the Receiving Party containing protections not materially less protective of the Confidential Information than those herein. Neither party will disclose the terms of these Terms or any Order Form to any third party other than its Affiliates, legal counsel, and accountants without the other party's prior written consent; provided that a party that makes any such disclosure to its Affiliate, legal counsel, or accountants will remain responsible for such Affiliate's, legal counsel's, or accountant's compliance with this "Confidentiality" section. Notwithstanding the foregoing: (i) ThreatMate may disclose the terms

of these Terms and any applicable Order Form to a subcontractor to the extent necessary to perform ThreatMate's obligations related to these Terms, under terms of confidentiality materially as protective as those set forth herein and (ii) ThreatMate may provide access to your Confidential Information to those of your Users, employees, contractors, and agents whom you permit to use and manage your access and use of the ThreatMate Cybersecurity Platform.

8.3. **Compelled Disclosure.** The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior 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 the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information.

9. **Representations, Warranties, and Disclaimers.**

9.1. **Representations and Warranties by you.** You represent and warrant to ThreatMate that: (a) you will abide by ThreatMate's Acceptable Use Policy (AUP) and (b) End User License Agreement (EULA). You further represent and warrant to ThreatMate that you will not, and will not authorize or induce any other party, to: (i) generate automated, fraudulent, or otherwise invalid reviews, questions, comments, lead conversions, clicks, or other actions with regard to the ThreatMate Cybersecurity Platform; (ii) use any automated means or form of scraping or data extraction to access, query, or otherwise collect ThreatMate Services or other data, content, or reviews from the ThreatMate Cybersecurity Platform, except as expressly permitted by ThreatMate; or (iii) use any ThreatMate trade or service marks in any manner without ThreatMate's prior written consent.

9.2. **Mutual Warranties.** Each party represents and warrants that it has the legal power to enter into these Terms.

9.3. **DISCLAIMER. Except as expressly provided herein, ThreatMate makes no warranty of any kind, whether express, implied, statutory, or otherwise, and ThreatMate specifically disclaims all implied warranties, including any implied warranty of merchantability, fitness for a particular purpose, non-infringement, uninterrupted or error-free use or service, error correction, availability, accuracy of informational content, system integration, and any and all implied warranties arising from statute, course of dealing, course of performance, or usage of trade, to the maximum extent permitted by applicable law. ThreatMate Services and the ThreatMate Cybersecurity Platform are provided "AS IS" and "AS AVAILABLE", exclusive of any warranty whatsoever. Furthermore, to the fullest extent permitted by law, ThreatMate specifically disclaims all warranties and guarantees regarding (a) performance, quality, and results, (b) click rates and conversions, and (c) the accuracy of the information that ThreatMate provides in connection with the ThreatMate Cybersecurity Platform and/or the ThreatMate Services. ThreatMate shall not be liable for non-performance of Subscribers or other third parties and non-performance due to causes beyond its reasonable control. Additionally, ThreatMate disclaims all liability arising from**

ThreatMate's access to your account on your behalf in order to make changes or post information to the ThreatMate Cybersecurity Platform in accordance with your instructions; it is your responsibility to confirm that your instructions are executed as requested. You acknowledge that ThreatMate does not control the transfer of data over telecommunications facilities, including the internet. ThreatMate does not warrant secure operation of the ThreatMate Cybersecurity Platform, ThreatMate Services, or any other third-party content and services made available on or through the ThreatMate Cybersecurity Platform (such as video conferencing or messaging services), or that it will be able to prevent disruptions to your access or use of the ThreatMate Cybersecurity Platform. You acknowledge further that the ThreatMate Cybersecurity Platform may be subject to limitations, delays, and other problems inherent in the use of the internet and electronic communications. ThreatMate is not responsible for any delays, delivery failures, or other damage resulting from such problems with the use of the internet or electronic communications.

10. **Data Protection.** The terms of the data processing addendum ("DPA"), made available to you via the ThreatMate Cybersecurity Platform, are hereby incorporated by reference and shall apply to the extent that you provide Personal Data (as defined in the DPA) to ThreatMate or its Affiliates, or ThreatMate transfers Personal Data, as part of your use of the ThreatMate Cybersecurity Platform.

11. Indemnification.

11.1. **Indemnification.** You will defend ThreatMate and its Affiliates against any claim, demand, suit, or proceeding made or brought against ThreatMate or any Affiliate arising out of or in connection with (a) a third party allegation that (i) your Content or Application infringes or misappropriates such third party's intellectual property rights, including rights of privacy and publicity (b) you have breached a contract or duty owed to another Subscriber (c) any violation of the representations and warranties provided under these Terms by you, (d) your and/or your Users' use of the ThreatMate Cybersecurity Platform or ThreatMate Services in an unlawful manner or in violation of these Terms and/or applicable Order Form ((a) through (c) each a "Claim Against ThreatMate"), and will indemnify ThreatMate and its Affiliates from any damages, attorney fees, and costs finally awarded against ThreatMate or its Affiliates as a result, or for any amounts paid by ThreatMate or its Affiliates under a settlement approved by you in writing, of a Claim Against ThreatMate, provided that ThreatMate: (i) promptly gives you written notice of the Claim Against ThreatMate; (ii) gives you sole control of the defense and settlement of the Claim Against ThreatMate (except that you may not settle any Claim Against ThreatMate unless it unconditionally releases ThreatMate and its Affiliates of all liability); and (iii) gives you all reasonable assistance, at your expense. The above defense and indemnification obligations do not apply if a Claim Against ThreatMate arises from ThreatMate's or its Affiliate's breach of these Terms (including the applicable Order Form).

11.2. **Exclusive Remedy.** This "Indemnification" section 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 claim for infringement, misappropriation, or otherwise.

12. Limitation of Liability.

12.1. Limitation of Liability. Except for each party's indemnification obligations under the "Indemnification" section, in no event shall the aggregate liability of either party, together with all of its affiliates, arising out of or related to these Terms exceed the total amount paid by you and your affiliates hereunder in the twelve months preceding the first incident out of which the liability arose. The foregoing limitation will apply whether an action is in contract or tort and regardless of the theory of liability but will not limit you and your affiliates' payment obligations under the "Fees and Payment" section above.

12.2. Exclusion of Consequential and Related Damages. In no event will either party or its affiliates have any liability arising out of or related to these Terms for any lost profits, revenues, goodwill, data, use, or other economic advantage, or for indirect, special, incidental, consequential, cover, business interruption, or punitive damages, whether an action is in contract or tort and regardless of the theory of liability, even if a party or its affiliates have been advised of the possibility of such damages or if a party's or its affiliates' remedy otherwise fails of its essential purpose. The foregoing disclaimer will not apply to the extent prohibited by law and does not limit either party's indemnification obligations under the "Indemnification" section or liability for first party infringement.

12.3. The parties agree that this section 10 represents a reasonable allocation of risk and that ThreatMate would not proceed in the absence of such allocation.

13. Non-Solicitation. You agree that you shall not, at any time during the term and for a period of 18 months after termination of these Terms, whether for your own account or for the account of others, solicit for employment, hire or otherwise engage any of the employees or independent contractors of ThreatMate. Notwithstanding the foregoing, nothing in these Terms shall prevent you from hiring any person who responds to a general solicitation not personally directed to such person. In the event you hire or engage an employee or contractor of ThreatMate in violation of this Section, ThreatMate shall be entitled to collect liquidated damages from you to compensate ThreatMate for locating, recruiting, hiring and training a replacement person. ThreatMate's liquidated damages shall be a sum equal to two times the gross annual compensation of the person you wrongfully hired or engaged. Gross annual compensation means twelve times the subject employee or contractor's last full month's compensation from ThreatMate including bonuses and benefits. The parties agree and acknowledge that this amount is a reasonable, liquidated amount and not a penalty.

14. General.

14.1. **Assignment.** Neither you nor ThreatMate may assign these Terms, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld); provided, however, that either of us may assign these Terms in their entirety (including all Order Forms), without the other party's prior written consent (a) to an Affiliate or (b) in connection with a change of control, merger, stock transfer, sale or other disposition of substantially all the assets of the assigning party's business. Subject to the foregoing, these Terms (including each Order Form) will bind and inure to the benefit of ThreatMate and you, and our respective successors and permitted assigns.

14.2. **Interpretation.** If any provision of these Terms or any applicable Order Form, shall be held to be invalid or unenforceable for any reason, the remaining provisions shall continue to be valid and enforceable. If a court of competent jurisdiction finds that any provision of these Terms or any applicable Order Form is invalid or unenforceable, but that by limiting such provision it would become valid or enforceable, then such provision shall be deemed to be written, construed, and enforced as so limited. Titles and headings of sections of these Terms are for convenience only and shall not affect the construction of any provision of these Terms. Any ambiguous provisions are not to be construed against either party. Any use of the term "include" or "includes" or "including" means "include without limitation," "includes without limitation" and "including," respectively.

14.3. **Relationship of the Parties.** You and ThreatMate are independent contractors to one another. These Terms do not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between us. Each of us will be solely responsible for payment of all compensation owed to our respective employees, as well as all employment-related taxes.

14.4. **Third-Party Beneficiaries.** There are no third-party beneficiaries under these Terms.

14.5. **Waiver.** No failure or delay by either of us in exercising any right under these Terms will constitute a waiver of that right.

14.6. **Export Compliance.** Each of us represents that it is not named on any U.S. government denied-party list. You will not permit any User to access or use the ThreatMate Cybersecurity Platform or any ThreatMate Services in a U.S.-embargoed country or region (currently Cuba, Iran, North Korea, Sudan, Syria, and Crimea) or in violation of any U.S. export law or regulation.

14.7. **Notice.** Unless otherwise expressly indicated, any consent or authorization required under these Terms shall be at the sole discretion of the party from whom such consent is required. Notice shall be deemed to have been received by a party, and effective, on the day received. All breach-related and indemnification-related notices permitted or required under these Terms shall be in writing and delivered by recognized postal or courier services who provide delivery confirmation to the other party's address set forth on the initial Order Form, or such other address as the parties may subsequently provide in writing. All other notices may be sent by email with notice deemed given: (a) upon acknowledgement of receipt by a reply email; or (b) when ThreatMate posts the notice in the ThreatMate Cybersecurity Platform.

14.8. **Force Majeure.** ThreatMate shall not be liable to you by reason of any failure in performance of these Terms if the failure arises out of the unavailability of communications facilities or energy sources, acts of God, your acts, acts of governmental authority, fires, strikes, delays in transportation, riots, terrorism, war, pandemics, cybersecurity incidents, or any other causes beyond the reasonable control of ThreatMate.

14.9. **Use by Foreign Nationals.** You will: (a) ensure that neither the ThreatMate Cybersecurity Platform nor any ThreatMate Services are used by any national (citizen or lawful permanent resident) of "Country Group E," as that term is defined by the U.S. Export Administration Regulations, 15 C.F.R. 740 et. seq.; and (b) not take any steps to facilitate such use.

14.10. **Applicable Law.**

14.10.1. **U.S., Canada, Caribbean and the Americas.** If your principal place of business (or primary residence, if you are an individual) is located in the United States, Canada, the Caribbean or anywhere else in North America, Central America or South America, these Terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in all respects (without regard to any conflict of laws provisions) in accordance with the laws of the United States of America and the State of Delaware as such laws are applied to agreements entered into and to be performed entirely within the State of Delaware.

14.10.2. **United Kingdom, Europe and Elsewhere.** If your principal place of business (or primary residence, if you are an individual) is located in the United Kingdom, Europe or anywhere other than North America or South America, these Terms and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with these Terms or their subject matter or formation shall be governed by and construed in all respects (without regard to any conflict of laws provisions) in accordance with the laws of England as such laws are applied to agreements entered into and to be performed entirely within England.

14.10.3. **Provisions Applicable in all Countries.** As these Terms are not a contract for the sale of goods, these Terms shall not be governed either by: (a) codification of Article 2 or 2A of the Uniform Commercial Code; or (b) the United Nations Convention on the International Sale of Goods. No version of the Uniform Computer Information Transactions Act shall apply to these Terms. ThreatMate and you confirm that we have requested that these Terms be drafted in English. Les parties contractantes confirment qu'elles ont exigé quele présent contrat et tous les documents associés soient redigés en anglais.

14.11. Dispute Resolution.

14.11.1. **Informal Resolution.** Subject to Section 14.11.6, ThreatMate and you agree to try for 60 days to resolve any dispute under or in connection with these Terms (a "Dispute") informally. If the parties cannot settle any Dispute during this time period, then subject to Section 14.11.6: (a) the parties agree to enter binding arbitration (as defined in this Section 14.11), and not to sue in court in front of a judge or jury; and (b) if your principal place of business is located in the United States, Canada, the Caribbean or anywhere else in North America, Central America or South America, the parties also agree that class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity are not allowed, nor is combining individual proceedings without the consent of all parties.

14.11.2. **Service of Process and Notice of Dispute.** To the fullest extent permitted by applicable law or by any rules of any applicable arbitrators, courts or other tribunals, both parties hereby designate each of their respective corporate officers (including the President, CEO, and other C-level executives or equivalents) as agents to receive service of process by delivery via a reputable overnight courier to the receiving party's address on file with the government registry of that party's jurisdiction of organization or formation. Each party hereby acknowledges and agrees that such service of process shall be adequate and sufficient as if it were made by formal service of process pursuant to applicable laws or rules.

If you wish to raise a Dispute and ThreatMate's customer service representatives cannot resolve it, a Notice of Dispute should be sent by postal mail to ThreatMate, ATTN: LEGAL DEPARTMENT, 8 The Green, Suite 14359, Dover, DE 19901 which includes: your name, address, how to contact your, the problem your wishes to raise, and your preferred means of resolution. ThreatMate will do the same if ThreatMate has a dispute with you. After 60 days, subject to Section 14.11.6, you or ThreatMate may start arbitration in accordance with Section 14.11.3 if the dispute is unresolved.

14.11.3. Exclusive Forum and Place of Arbitration.

14.11.3.1. **U.S., Canada, Caribbean and the Americas.** If your principal place of business (or primary residence, if you are an individual) is located in the United States, Canada, the Caribbean or anywhere else in North America, Central America or South America, and a Dispute was not resolved through the informal resolution process described above then, subject to Section 14.11.6: (a) such Dispute shall be finally settled in accordance with the Commercial Arbitration Rules of the American Arbitration Association; and (b) any such arbitration shall be conducted in the English language in Anne Arundel County, Maryland by a sole arbitrator.

14.11.3.2. **United Kingdom, Europe and Elsewhere.** If your principal place of business (or primary residence, if you are an individual) is located in the United Kingdom, Europe or anywhere other than North America, Central America or South America, and a Dispute was not resolved through the informal resolution process described above then, subject to Section 14.11.6: (a) such Dispute shall be finally settled in accordance with the Rules of Arbitration of the International Chamber of Commerce, as amended by this section 14.11; and (b) any such arbitration shall be conducted in the English language in London, England by a sole arbitrator.

14.11.4. **Appointment of Arbitrator.** For the purposes of the arbitration, a single arbitrator shall be selected by the parties, in default of which the arbitrator shall be appointed in accordance with the applicable arbitration rules. The arbitrator elected by the parties must be a qualified attorney, solicitor or barrister with at least 10 years of post-qualification practice experience, and also have experience in the fields of software development and distribution and intellectual property disputes (together, the "Requirements"). In appointing an arbitrator, the arbitral tribunal must, as far as possible, have regard to the Requirements.

14.11.5. **Limitations.** To the extent permitted by applicable law, you must commence arbitration of any Dispute within one year of the date on which the relevant cause of action accrued (or, if later, within one year of the date on which the innocent party ought reasonably to have become aware of such an accrual), otherwise it is permanently barred. The arbitrator shall be bound by the provisions of these Terms and base the decision on applicable law and judicial precedent, shall include in such decision the findings of fact and conclusions of law upon which the decision is based, and shall not grant any remedy or relief that a court could not grant under applicable law. Except to the extent otherwise expressly provided in applicable arbitration rules, the arbitrator's decision shall be final and binding upon the parties, and shall not be subject to appeal.

14.11.6. **Enforcement; Equitable Relief; IP Disputes.** Notwithstanding anything to the contrary in this Section 14.11: (a) either party may enforce any judgment rendered by the arbitrator in any court of competent jurisdiction; (b) the arbitrator shall have the right to issue equitable relief, including preliminary injunctive relief; (c) ThreatMate shall be entitled to apply to any court of competent jurisdiction for any interim relief; (d) ThreatMate shall be entitled to bring, in any court of competent jurisdiction, at any time, any claim concerning or related to the enforcement or validity of any intellectual property rights (including, for the avoidance of doubt, any trade secrets or confidential information) of ThreatMate or licensors of ThreatMate (an "IP Dispute"); and (e) ThreatMate shall be entitled, upon receipt of any request for arbitration from your under this Section 14.11, to decline to submit to the jurisdiction of any arbitral tribunal insofar as the request for arbitration relates to any IP Dispute, in which case you may bring the same IP Dispute in any court of competent jurisdiction.

14.11.7. **Attorneys' Fees.** The rules of the applicable arbitral tribunal will govern payment of filing fees and the arbitrator's fees and expenses, but the prevailing party shall be entitled to recover reasonable attorneys' fees and costs.

14.12. Changes in Laws. Notwithstanding anything to the contrary in these Terms, ThreatMate may limit or discontinue the provision of the ThreatMate Cybersecurity Platform and ThreatMate Services to the extent: (a) ThreatMate or any vendor of ThreatMate is restricted by any rule, regulation, law or governmental entity; (b) ThreatMate or any vendor has discontinued the collection of data; or (c) ThreatMate or any vendor of ThreatMate is prohibited from providing Services. In addition, ThreatMate may discontinue, upgrade or change the production, support, delivery and maintenance of the ThreatMate Cybersecurity Platform and any ThreatMate Services if ThreatMate develops an upgraded version or otherwise no longer generally provides the same to its subscribers. In the event that ThreatMate materially modifies the content or scope of the ThreatMate Cybersecurity Platform of ThreatMate Services provided to you, the parties shall renegotiate the fees in good faith according to the prevailing pricing models.

14.13. Forms of Consent. These Terms (including applicable Order Forms) and any amendments thereto may be executed in counterparts. **The parties consent to the conduct of transactions and the execution of any amendments between them by electronic means or records, including by use of electronic signatures and facsimile copies of a party's signature.**

14.14. Entire Agreement. Some of the ThreatMate Services may be subject to additional terms and conditions, including our Acceptable Use Policy ("Additional Terms"), which are posted separately from these Terms but are incorporated and form a part of these Terms if you decide to use or access those features. These Terms (including the then-current Website Terms of Use, any applicable Additional Terms, and the other components identified in the Introduction) contain the entire agreement of the parties with respect to the subject matter hereof, and there are no other promises or conditions in any other agreements, whether oral or written. These Terms supersede any prior written or oral agreements between the parties in connection with the subject matter hereof. The parties agree that any term or condition stated in a purchase order provided by you or in any other order documentation provided by you (excluding Order Forms) is void and expressly rejected. In the event of any conflict or inconsistency, the order of precedence shall be: (a) the applicable Order Form, (b) any applicable Additional Terms, (c) these Terms, and (d) the Website Terms of Use. ThreatMate reserves the right, in its sole discretion, to change terms and conditions of any of the exhibits – including the General Terms and Conditions in Exhibit A ("Updated Terms") from time to time. Unless ThreatMate makes a change for legal or administrative reasons, ThreatMate will provide reasonable advance notice before the Updated Terms become effective. You agree that ThreatMate may notify you of the Updated Terms by posting them on the ThreatMate Cybersecurity Platform, and that your use of the ThreatMate Cybersecurity Platform after the effective date of the Updated Terms (or engaging in such other conduct as ThreatMate may reasonably specify) constitutes your agreement to the Updated Terms. You should review these Terms and any Updated Terms before using the ThreatMate Cybersecurity Platform or any ThreatMate Services. The Updated Terms will be effective as of the time of posting, or such later date as may be specified in the Updated Terms, and will apply to your use of the ThreatMate Cybersecurity Platform and the ThreatMate Services from that point forward. Except as otherwise expressly provided in this Section, these Terms may be amended or modified only in a writing executed by both parties.

Exhibit B – Definitions

"Acceptable Use Policy" means ThreatMate's then-current conditions for remote access to any ThreatMate asset, including the ThreatMate website and the ThreatMate Cybersecurity Platform website platform.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Channel Partner" means a Subscriber who is a managed services provider, value-added reseller, consultant, IT service provider or other member of the information technology channel

community. Use of the term "partner" in this context is used in the colloquial sense; these Terms do not create or constitute a legal partnership between or among ThreatMate or any Channel Partner, Vendor or other Subscriber.

"ThreatMate" means ThreatMate Inc. and/or its Affiliates, as identified in the relevant Order Form.

"ThreatMate Services" means the content and information created, and those services, tools or functionalities offered, by ThreatMate, its Affiliates, or their respective licensors that are made available to you on or through the ThreatMate Cybersecurity Platform, and all associated features and dashboards. ThreatMate Services includes but is not limited to the Channel Pitch, Channel Explorer, Channel Command, Channel Chatter and Channel Cash, infographics, research insights, various means of communication or interaction with Vendors, Vendor management tools, and/or social media assets.

"ThreatMate Cybersecurity Platform" means the website(s) and mobile application(s) owned and operated by ThreatMate and/or its Affiliate(s) at which, among other things MSPs and their Users as potential purchasers of business solutions and services may view or access ThreatMate Services. The ThreatMate Cybersecurity Platform includes ThreatMate Services.

"Malicious Code" means code, files, scripts, agents or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

"Order Form" means any printed or electronic ordering or registration document or page, including, in either case, any addenda and supplements thereto, which cross-references and is subject to these Terms. By entering into an Order Form, you and your Affiliates agree to be bound by these Terms as if each were an original party to these Terms.

"Subscriber" or **"you"** or **"your"** means, in the case of an individual accepting these Terms on their own behalf, such individual, or, in the case of an individual accepting these Terms on behalf of a company or other legal entity, the Company Subscriber for which such individual is accepting these Terms and the Affiliates of that Company Subscriber (for so long as they remain Affiliates). Depending on the applicable Subscription Level, a Subscriber may act in the capacity as (a) a Vendor wishing to promote products or services or (b) a Channel Partner wishing to promote a sales channel.

"Subscription Level" means the level of ThreatMate Services to which you are then subscribed, based either on the subscription level to which you subscribed during the registration process or thereafter.

"User" means an individual who you, as a Company Subscriber, authorize to use your ThreatMate Cybersecurity Platform account, and to whom you (or, when applicable, ThreatMate at your request) have supplied a user identification and password. Users may (a) include your employees, consultants, contractors and agents, and third parties with which you transact business, each of whom is acting solely on or for your behalf, and with your express permission, and (b) be limited by Subscription Level.

“Vendor” means a Subscriber who is an information technology vendor or distributor, including any Subscriber which provides Applications or Subscriber Content featured, listed, described or made available on or through the ThreatMate Cybersecurity Platform.

“Vendor Application” means any Vendor product or service, including any business solution, web-based, mobile, offline, cloud-based or other application or software that may be featured, listed, described or made available on the ThreatMate Cybersecurity Platform.

“Subscriber Content” means any content or information provided by a Vendor or another Subscriber that is made available to you on or through ThreatMate Cybersecurity Platform. Subscriber Content includes content or information about Applications provided by Vendors, and may include content in any form, including in the form of text, documents, graphics, audio or videos.

“you” or your” or “**Subscriber”** means, in the case of an individual accepting these Terms on their own behalf, such individual, or, in the case of an individual accepting these Terms on behalf of a company or other legal entity, the Company Subscriber for which such individual is accepting these Terms and the Affiliates of that Company Subscriber (for so long as they remain Affiliates). Depending on the applicable Subscription Level, a Subscriber may act in the capacity as (a) a Vendor wishing to promote products or services or (b) an Channel Partner wishing to promote a sales channel.

“your Content” means any content, data, information, or other materials which you embed or post, or otherwise make available or generate on the ThreatMate Cybersecurity Platform.

****

Data Protection Addendum

This Data Protection Addendum (“DPA”) is made a part of your Subscriber Terms of Use (“Terms”), and governs solely to the extent that: (a) you, or any person (“Person”) from whom ThreatMate collects Personal Data (defined below), is located in the European Economic Area (“EEA”) or the United Kingdom ("UK"); (b) you and/or such Person is subject to Data Protection Laws (defined below); and (c) your access and use of the ThreatMate Cybersecurity Platform involve the collection or processing of the Personal Data of an individual located in the EEA or the UK. To the extent this DPA applies, and in consideration of the mutual obligations set out in this DPA, you and ThreatMate agree that this DPA is a binding part of the Terms.

Except as modified in this DPA, the terms and conditions of the Terms shall remain in full force and effect. If there is any conflict between this DPA and the Terms regarding ThreatMate’s privacy or security obligations, the provisions of this DPA shall control. Unless expressly

defined in the DPA, all capitalized terms used herein will have the meaning assigned to them in the Terms.

Purpose: The purpose of compliance with Data Protection Laws concerning the processing of Personal Data on behalf of ThreatMate Cybersecurity Platform users located in European Union ("EU") Member States or members of the European Economic Area and incorporates (to the extent applicable) the terms of the EU Standard Contractual Clauses ("SCCs"). "Data Protection Law" means, where applicable, the European General Data Protection Regulation (EU 2016/679) ("GDPR"), including applicable laws implementing or supplementing the GDPR and as transposed into domestic legislation of Member States, as amended, replaced or superseded from time to time) and the UK Data Protection Act of 2018. The terms Processor, Controller, processing (and process), personal data breach, data protection impact assessment and Personal Data shall have the meanings set out in Data Protection Laws. The term "Personal Data" includes: first and last name, email address, telephone number, mailing address, and other information necessary to identify an individual for purposes of assisting ThreatMate with providing use of the ThreatMate Cybersecurity Platform.

Context and Scope of Personal Data Processing: In order to provide the Vendors or Subscribers with access and use of the ThreatMate Cybersecurity Platform, it may be necessary for ThreatMate to collect Personal Data of such an individual or an employee or other representative of the Vendor or Subscriber (each, a "Customer Representative"). Such data is collected when Customer Representatives provide their Personal Data directly to ThreatMate as an account holder or a designated point of contact between Vendor or Subscriber and ThreatMate. That data is subsequently used by ThreatMate solely to provide access to the ThreatMate Cybersecurity Platform and the ThreatMate Content and Services under the Terms, or as may be necessary to assist with any requests regarding use and proper operation of the ThreatMate Cybersecurity Platform.

Obligations under Data Protection Laws:

1. Processing as a Controller. Generally, ThreatMate shall act as the Controller of the Personal Data of each Customer Representative. As a Controller, ThreatMate will comply with all data protection requirements under the Data Protection Laws applicable to the Personal Data. Without limiting the foregoing, as a controller of the Personal Data, ThreatMate shall be responsible for providing notifications to, and respond to inquiries and requests from, the Customer Representatives; provided, however, that to the extent necessary, the Vendor or Subscriber, as applicable, shall reasonably cooperate with ThreatMate for the purpose of responding to requests by Customer Representatives or any government authorities and of generally complying with ThreatMate's obligations

under the Data Protection Laws. To the extent applicable, nothing herein relieves the Vendor or Subscriber of their own obligations under the applicable Data Protection Laws. The parties are not entering a relationship of joint controllership.

1. Processing as a Processor. In the event any personal data is processed by ThreatMate as a Processor, the parties shall specifically identify such personal data and the purposes of processing, as well as the measures undertaken to protect such data, by completing Appendix B (Controller-to-Processor). As a Processor, ThreatMate shall only process Personal Data in accordance with the Customer Representative's documented instructions. As required under Data Protection Laws, ThreatMate shall assist the Customer Representative, where appropriate, in ensuring compliance with the Customer Representative's obligations pursuant to Data Protection Laws, taking into account the nature and scope of ThreatMate's Personal Data processing, which may include providing commercially reasonable cooperation and assistance with: (a) data subject requests (see below); (b) notifications or communications regarding personal data breaches; (c) data protection impact assessments; and (d) prior consultations with supervisory authorities.

With respect to any Personal Data processed by ThreatMate as a Processor pursuant to this DPA, ThreatMate shall: (a) in the event ThreatMate engages trusted third parties to process Personal Data ("Trusted Parties"), seek the prior specific or general written authorization of the Controller, which is hereby given in respect of any Trusted Parties expressly listed below (and in the case of general written authorization, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of Trusted Parties, thereby giving the Controller the opportunity to object to such changes); (b) unless prohibited under applicable law, upon termination of the Services, at its option, either return or destroy the Personal Data (including all copies of it); (c) ensure that all persons authorized by ThreatMate to access the Personal Data on ThreatMate's behalf, are subject to obligations of confidentiality in accordance with confidentiality obligations set forth in the Terms; (d) remain fully liable to the Customer Representative, Vendor, or Subscriber for the failure of those persons authorized by ThreatMate to access the Personal Data on ThreatMate's behalf; and, (e) make available such information as may be necessary to demonstrate compliance with its obligations under Article 28 of the GDPR and will (at the Customer Representative's cost and expense) contribute to and allow for appropriate reasonable audits.

The Trusted Parties currently engaged to process Personal Data on behalf of ThreatMate include HubSpot, Google (Google Analytics), and YouTube, Inc.

Security: ThreatMate limits its collection of Personal Data to only that which is relevant for purpose of providing the services under the Terms and retains Personal Data in a form that permits identification of data subjects (defined below) for no longer than is necessary to serve that purpose. ThreatMate maintains a retention register documenting the regulatory, statutory

and business retention periods which it applies to its records. Where no defined or legal retention period exists, the default standard retention period is six (6) years plus the year in which the record was created. ThreatMate shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. ThreatMate currently employs multi-factor authentication as a technical and an organizational measure.

Data Subject Rights: Within the scope of Data Protection Laws, Customer Representatives located in the EEA or the UK ("data subjects") have certain rights that they may exercise, based on jurisdiction, in relation to the processing of their Personal Data. Where applicable, these rights include: the right to access, correct, update, and delete that data subject's Personal Data, to withdraw any consent to processing, to opt out of communications, to restrict processing of Personal Data, and to make any claim or complaint in relation to their rights under Data Protection Laws, ThreatMate shall respond to and offer reasonable assistance in responding to data subjects' requests to exercise their data protection rights in accordance with applicable Data Protection Laws**.**

EU Standard Contractual Clauses

1. **Controller-to-Controller**: Generally, and unless otherwise specifically identified in Appendix B (Controller to Processor) of this Addendum, all transfers of Personal Data from Vendor or Subscriber to ThreatMate shall be deemed a controller-to-controller transfer and shall be made pursuant to Module 1 of the Standard Contractual Clauses adopted by the European Commission on June 4, 2021, as currently set out at in the Annex at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en (collectively, the " Controller SCCs").

1. **Controller-to-Processor:** Where Personal Data is transferred from Vendor or Subscriber to ThreatMate on a controller-to-processor basis as specifically set forth in Appendix B (Controller to Processor) of this Addendum, the transfer shall be made pursuant to Module 2 of the Standard Contractual Clauses adopted by the European Commission on June 4, 2021, as currently set out in the Annex at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en (collectively, the " Processor SCCs").

The parties agree to observe the terms of the Processor SCCs without modification, except as to the following selections:

- In connection with Module 2, Option 2 of Clause 9(a) (Use of sub-processors) is selected and the applicable time period shall be 30 days.
- Clause 11(a) (Redress) does not select the Option.
- Clause 13(a): The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
- In Clause 14 (Local laws and practices affecting compliance with the Clauses), the provisions for Module 3 shall have no effect, and are hereby deemed deleted.
- In Clause 15 (Obligations of the data importer in case of access by public authorities), the provisions for Module 3 shall have no effect, and are hereby deemed deleted.
- In Clause 16 (Non-compliance with the Clauses and termination), the provisions for Module 4 shall have no effect, and are hereby deemed deleted.
- In Clause 18 (Choice of forum and jurisdiction), the selection in subclause (b) shall be Ireland.

In the event of inconsistencies between the provisions of the SCCs and this DPA or other agreements between the parties, the SCCs shall take precedence. The terms of the DPA shall not vary the SCCs in any way. The execution and delivery of this Addendum shall be deemed execution and delivery of the applicable SCCs. The governing law of any applicable SCCs shall be the Member State in which the Vendor or Subscriber (as Data Exporter) is established, or, if applicable, the UK. Each of the parties' signatures, authentications, or consents to the Terms shall be considered applicable to the DPA and SCCs as well. If so required by the laws or regulatory procedures of any jurisdiction, the parties shall execute or re-execute the SCCs as separate documents setting out the proposed transfers of Personal Data in such manner as may be required.

****

Page Break

APPENDIX A (CONTROLLER-TO CONTROLLER)

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

Data importer(s):

1. Name: ***ThreatMate***

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Representatives of Data Exporter

Categories of personal data transferred

First and last name, email address, telephone number, mailing address, and other information necessary to identify an individual for purposes of assisting ThreatMate with providing use of the ThreatMate Cybersecurity Platform

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed

specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous basis

Nature of the processing

Collection, recording, storage, backup and all other processing required for the functioning of the Data Importer's platform and the provision of Data Importer's services to the Data Exporter

Purpose(s) of the data transfer and further processing

To enable Data Exporter's Use of the Data Importer's service and platform

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period will be for the duration of the services provided by Data Importer to Data Exporter and for any additional period necessary for Data Importer to maintain its backup data, to comply with legal requirements (including tax reporting purposes), and/or to assert or defend its legal rights in connection with Data Importer's business relationship with the Data Exporter

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

All processing required for collecting, handling, and otherwise processing personal data to enable Data Importer to provide the services and the platform to Data Exporter

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Ireland

Page Break

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

All (sub-) processors are required to provide measures at least as protective as the measures provided by the Data Importer

Page Break

APPENDIX B (CONTROLLER TO PROCESSOR)

[If applicable, complete duplicate information from Appendix A for Controller-to-Processor transfers]