ARTIFICIAL INTELLIGENCE USE ADDENDUM

This Artificial Intelligence Use Addendum ("AI Addendum") is made a part of the Agreement (defined below) between Customer (**"Customer," "You" or "Your"**) and Company ("**We," "Us," or "Our"**) under which Company provides the Customer with Products and Services (the "Agreement"). Company and Customer may each be referred to in this Agreement as a "Party" or together as the "Parties."

Background

We may use artificial intelligence (AI) tools in connection with the delivery of Our Products and Services. As applicable, We undertake to use only those artificial intelligence tools that comply with Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence ("EU AI Act").

Definitions

For the purpose of this AI Addendum, the terms "AI System," "Deployer," "Provider," "High Risk System," "General-Purpose AI (GPAI) model" and "Serious Incident" shall have the meanings given to those terms under the EU AI Act.

"Agreement" means the written or electronic agreement between Customer and the applicable Company entity for the provision of Products and/or Services to Customer, including but not limited to the End User License Agreement ("EULA," available at https://www.trellix.com/assets/legal/trellix-eula.pdf), Customer Data Processing Agreement, cloud terms of service agreement, professional services terms, technical support and maintenance service terms, or any other agreement between Customer and the applicable Company entity, each of which shall be deemed to incorporate this AI Addendum. In the event of a conflict between the terms of this AI Addendum and the Agreement, the terms of this AI Addendum will control.

"AI Features" means Company solutions, including Trellix Wise, that use Artificial Intelligence (AI) or Machine Learning (ML) to analyze telemetry data received from customer networks and devices worldwide to identify patterns and anomalies that may suggest malicious activity, and to proactively and adaptively investigate and respond to threats in real-time.

"Applicable Regulations" means the applicable country, federal, state data protection, privacy and artificial intelligence laws including but not limited to, the General Data Protection Regulation (GDPR), and the EU AI Act, as each may be adopted or amended from time to time.

"Automated Decision Making Technology" means any technology that processes personal information and uses computation to replace or substantially replace human decision-making.

"Company" means one of the following legal entities with whom Customer has contracted for Products and/or Services: (a) Musarubra US LLC, (b) Musarubra Ireland Limited; (c) Musarubra Japan KK, (d) Trellix (Beijing) Security Software Co. Ltd, (e) Musarubra Singapore Pte Ltd, (f) Musarubra Australia Pty Ltd, and (g) Trellix Public Sector LLC.

"Customer Data" means information collected from the Customer including system information, IP addresses, email addresses, host names, file paths, log information, that is not aggregated, anonymized or pseudonymized, where appropriate.

"Input" means any information, prompts, inquiries, documents, or any type of data directly provided to the AI System on the basis of which the system produces an Output.

"Output" means any response, predictions, content (including text, images, photos, videos, graphics or other files), recommendations, remediations, suggestions or decisions generated by the AI System or AI Features.

"Third Party AI Features" means any third party integration or functionality that uses Artificial Intelligence (AI) or Machine Learning (ML) to assist in the provision of Our Products and Services.

"Threat Data" means non-personally identifying and non-Customer identifying information about Malware, threats, actual or attempted security events, including but not limited to their frequency, source, associated code, general identifiers, attacked sectors and geographies.

For purposes of the EU AI Act, Customer is a "Deployer" and Company is a "Provider" of an AI System. The parties will fulfill their respective obligations under the EU AI Act, and any other applicable laws or regulations that may come into force that apply to Our use of artificial intelligence.

Capitalized terms used but not otherwise defined in this AI Addendum have the meanings set forth in the EULA.

1. **Use of Artificial Intelligence**

1.1 **Use of AI in Product and Services**. We may provide You with AI Features which may include tools to analyze telemetry data received from customer networks and devices worldwide to identify patterns and anomalies that may suggest malicious activity, and to proactively and adaptively investigate and respond to threats. You may provide Input into the AI Features and receive Output generated and returned by the AI Feature based on the Input. By using AI Features, You acknowledge and agree to the sharing of Your Input with Us and the potential risks associated with such data sharing. You assume sole and exclusive responsibility with respect to the Input that You share. To the extent permitted by law, We shall have no responsibility or liability regarding the Input or Your use of the Output.

1.2 **Cybersecurity Purposes.** We do not engage in activities that are deemed "high risk" under applicable regulations, including the EU AI Act. Our AI Features are not used in a way that could fundamentally violate human rights or manipulate human behavior, allow social scoring, or make automated decisions that could result in discrimination. Our AI Features are intended to be used solely by our customers' security analysts to detect, manage and respond to potential cybersecurity threats, and for no other purposes. For these limited cybersecurity purposes, we provide General Purpose AI (GPAI) models to assist our customers' security analysts in detecting, managing and responding to potential cybersecurity threats. Even though the use of Our AI Features is itself not high risk, we recognize that many customers do themselves engage in high risk activities, including the management or support of critical infrastructure, and the processing of highly sensitive data. We also recognize that Our solutions are integral to our customers' overall security posture and commit to regular monitoring of AI Features. Your use of Our Products, Services or Software as part of a "high risk" AI System is at Your sole discretion. You are solely responsible for Your use of the AI Features in accordance with applicable laws and standards, and Your decisions, actions and omissions in reliance or based on Outputs.

1.3 **Use of AI in Internal Operations.** Our employees and contractors may use AI tools internally to support service delivery, software development, client communications, and administrative functions. When doing so, all Company personnel are required to comply with Company's standard internal AI use policies.

1.4 **Third Party AI Providers.** Our Products may incorporate Third Party AI Features. By choosing to use Third Party AI Features, You acknowledge and agree to the sharing of your Input with Third Party AI Features providers. We maintain contractual agreements with Third Party AI providers and endeavor to impose substantially similar appropriate contractual obligations in writing upon Third Party AI Providers that are no less protective than the obligations set forth in this agreement and Our Supplier Data Processing and Security Agreement and Our Supplier Security Addendum. Third Party AI Features may be subject to additional third-party terms different than the Agreement. You agree to comply with such third-party terms, as such third-party terms may be updated, modified, or added from time to time.

1.5 **Ownership of Inputs and Outputs.** You provide the Inputs based on Your usage of Our Products and Services. We retain all right, title and interest in the Outputs, and nothing in the Agreement transfers to Customer any ownership interest in the Outputs. You understand that in some cases Output may be in the form of Threat Data.

1.6 **Limited Data Use.** Our AI System and AI Features are designed to adapt and learn from customer environments and event data, including through automated learning, to improve the security outcomes We provide to You. Customer Data is used only for legitimate cybersecurity purposes as contemplated under the Agreement. We implement comprehensive data quality checks to ensure the accuracy, completeness and consistency of datasets. We curate data sets to be relevant to the intended purpose of the AI System. We collect data lawfully and ethically, adhering to applicable data protection, privacy and artificial intelligence regulations. We use anonymization and pseudonymization techniques where appropriate.

1.7 **Accuracy and Errors.** We acknowledge the importance of ensuring that the AI System has a sufficient level of accuracy, reliability and comprehensiveness to deliver the Products and Services under the Agreement. We will (a) take all reasonable measures to mitigate the risks of Errors in the ongoing use of the AI System, and (b) regularly monitor and assess the AI System for Errors. For purposes of this Agreement, "Error" means any inaccuracy or error in the underlying AI System that may cause a risk of serious harm to the business or reputation of the Customer. In the event that possible Errors in the AI System are identified, We will (at no additional charge) notify You, and investigate and take appropriate remedial actions to rectify or mitigate such Errors.

1.8 **Feedback.** We own and retain all right, title and interest (including all intellectual property rights) in and to the AI System and AI Features. Any feedback or suggestions that You provide to Us regarding any Company Products or Services is non-confidential and may be used by Us for any purpose without acknowledgement or compensation; provided, however, You will not be identified publicly as the source of the feedback or suggestion.

1.9 **Human Oversight.** We will implement mechanisms for appropriate human oversight of the AI System, including regular reviews by subject-matter experts to help ensure that the AI System operates within ethical and applicable regulatory boundaries.

1.10 **Human-in-the-Loop.** To the extent required by applicable law or regulation, if You decide to use any Output to assist in making any automated decision that has significant consequences for an individual's life, well-being or fundamental human rights, You agree that You will implement meaningful human oversight.

2.0 **Monitoring.**

2.1 **Transparency, Explainability and Interpretability.** We will provide to You appropriate technical documentation (e.g., model cards, data sheets, fact sheets) sufficient to fulfill Our transparency obligations under Applicable Regulations, when appropriate. Notwithstanding any transparency requirements, all proprietary Threat Data, algorithms, and model weights remain as Our exclusive intellectual property. You shall not attempt to re-identify any de-identified threat data or reverse-engineer AI models relating to our AI System or AI Features. You agree that Our obligation to provide transparency does not extend to the disclosure of specific Threat Data used for training, proprietary model weights, or raw code. Disclosure of such items is deemed "not proportionate" for transparency and would constitute a breach of Company trade secrets.

2.2 **Transparency Compliance.** The technical documentation provided under Section 2.1 is intended to satisfy Customer's obligation to provide "meaningful information about the logic involved" in Automated Decision Making Technology. You agree that the disclosures in Section 2.1 are sufficient and that We are not required to provide raw training data or specific "weights" to satisfy a consumer's request for information.

2.3 **Risk Management System.** We will maintain a risk management system to include proactive identification of risks to safety and fundamental rights, assessment of the severity and probability of

identified risks, and reasonable technical and organizational measures to reduce risk to an acceptable level.

2.4 **Regulatory Inquiries.** We will cooperate with You without undue delay, in responding to any regulatory inquiries, audits, or other requests received from or commenced by any governmental body, standards body, or similar entity relating to Our AI models and their operations.

2.5 **Changes to AI System**. We may make changes to the AI System or AI Features, at any time, without notice to You and without Your consent, for the general benefit of Our customers that use the AI System or AI Feature.

3.0 **Security Measures.** In accordance with Applicable Regulations, We implement technical and organizational measures intended to provide a level of security appropriate to the risks presented by the development and use of the AI System and AI Features in our Products and Services.

4.0 **Compliance with Copyright Law.** We do not warrant that AI-generated Inputs or Outputs are free from third-party intellectual property claims. You will ensure any Input is free from any claim of copyright to Input data. You assume all responsibility for reviewing AI Inputs for potential intellectual property infringement prior to use of AI System or AI Features. You will hold us harmless from all claims, suits, demands, and proceedings alleging, claiming, seeking, or asserting any liability, loss, obligation, risk, cost, damage, award, penalty, settlement, judgment, fine, or expenses (including attorneys fees) arising from a claim that Your use of Our AI System or AI Features infringes any copyright, trademark or other purported intellectual property right.

5.0 **AI System Incidents.** Each Party shall notify the other without undue delay, and in any event within seventy-two (72) hours, of becoming aware of any “serious incident” as defined in the EU AI Act.

5.1 **Cooperation for Regulatory Reporting.** You shall provide Us with technical logs and a detailed description of the incident context to enable Us to establish a causal link as required for applicable regulatory reporting.

5.2 **Corrective Actions.** We may suspend AI Features if We determine a "reasonable likelihood" of a link between the AI Features and a serious incident until remedial actions are implemented.

6.0 **Disclaimer.** THE AI SYSTEM AND AI FEATURES ARE PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS. WE AND THE APPLICABLE THIRD-PARTY AI FEATURE PROVIDERS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE OPERATION OF THE AI SYSTEM OR AI FEATURES, OR THE INFORMATION, TEXT, AND CONTENT INCLUDED IN THE OUTPUT, OR THE USE OF THE INPUT, INCLUDING WITHOUT LIMITATION, ACCURACY OF THE RESULTS, OUTPUT, AVAILABILITY, SUITABILITY, RELIABILITY, OR CONTENT OF ANY INFORMATION PROVIDED THROUGH THE AI SYSTEM OR AI FEATURES. COMPANY WILL HAVE NO LIABILITY OR RESPONSIBILITY ARISING IN ANY WAY FROM CUSTOMER USE OF THE AI SYSTEM OR AI FEATURES; AND THE CUSTOMER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE AGGREGATE LIABILITY UNDER THIS AI ADDENDUM SHALL NOT EXCEED THE TOTAL FEES RECEIVED BY US FOR THE APPLICABLE PRODUCTS AND SUPPORT PURCHASED UNDER THE TERMS OF THIS AGREEMENT AND ATTRIBUTABLE TO THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO SUCH LIABILITY. THE LIMITATIONS IN THIS SECTION APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

7.0 **Additional Use Restrictions.** In addition to the use restrictions described in the Agreement, including Section 2.6 General Restrictions of the EULA, You shall not, directly or indirectly, and shall not permit any third-party to: (a) access or use the AI Features or its Output to develop, train,

or improve any other solutions or models that use Artificial Intelligence or Machine Learning; (b) engage in model extraction, or otherwise attempt to derive or gain access to any source code, algorithm, model, model weights and parameters, or other underlying technology or component of the AI Features, in whole or in part; (c) perform prompt injection attacks; (d) use the AI Features to create or generate an Output or use an Output in a manner that You know or should know infringes, misappropriates, or otherwise violates any intellectual property right or other right of any person or violates any applicable laws; or (e) input or otherwise process any personally identifiable information through the AI Features without appropriate prior authorizations.

-End-