CUSTOMER DATA PROCESSING AGREEMENT

This Customer Data Processing Agreement ("**DPA**"), including *Exhibits A and B*, is made a part of the Agreement (defined below) between Customer ("**Customer**," "You," or "Your") and Company (defined below, "**Company**," "We," "Us," or "Our"). Company and Customer may each be referred to in this DPA as a "Party" or together as the "Parties." All capitalized terms not expressly defined in this DPA shall have the same meaning ascribed to them in the applicable Agreement(s) between Customer and Company.

RECITALS

WHEREAS, Your contractual counterparty for the purposes of this DPA will be the Company entity with whom You have contracted for Company's Products and Services;

WHEREAS, Company's provisioning of its Products and Services to Customer may involve cross-border Transfers;

WHEREAS, Company has implemented "follow the sun" support operations to ensure 24/7 support, with support teams in various locations worldwide, including the U.S. and India;

WHEREAS, 'On-premises' Company Products are configured by the Customer and any transmission to the Company of Customer's Personal Data is determined *solely* by the Customer; and

WHEREAS, Company does not voluntarily permit the United States Government or other governmental agencies access to Company's infrastructure.

1. DEFINITIONS

For the purposes of this DPA, "**Processing**," "**Controller**," "**Data Subject**", "**Sub-processor**," "**Commission**," "**Member State**," "**Processor**," and "**Supervisory Authority"** shall have the same meanings ascribed to them by the GDPR or other Applicable Laws.

"**Business**," "**Service Provider**," and "**Consumer**" shall have the meaning ascribed to such terms per the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100, et seq., ("**CCPA**").

"**Affiliates**" means any entity that directly or indirectly controls, is controlled by, or is under direct or indirect common control with, or has the same parent entity, with an entity that is a Party to this DPA or one or more of the other Affiliates of that entity (or a combination thereof). For the purpose of this definition, an entity controls another entity if and as long as the first entity owns, beneficially or of record, more than fifty percent (50%) ownership interest in the other entity.

"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"), 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 DPA.

"**Applicable Laws**" means the applicable country, federal, state data protection and privacy law including but not limited to, the GDPR, the CCPA, the Swiss Federal Act on Data Protection,

and the United Kingdom Data Protection Act 2018, as each of the above as may be amended from time to time.

"**Company"** means one of the following legal entities with whom Customer has contracted for Company 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.

"**Confidential Information**" has the same meaning as set forth in the Agreement.

"**GDPR**" means, as applicable: (a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**EU GDPR**"); and/or (b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as it forms part of the laws of the United Kingdom ("**UK GDPR**") as each may be amended from time to time.

"**Personal Data**" means "Personal Data," or "Personal Information" as defined under Applicable Laws that the Company collects or receives on Your behalf. Personal Data does not include Personal Data or Personal Information that We obtain or Process independent of the performance of Our obligations under the Agreement with You.

"**Personal Data Breach**" means (a) with respect to Personal Data subject to the GDPR, a "Personal Data Breach" as defined in the GDPR, and (b) with respect to Personal Data subject to Applicable Law other than the GDPR, a security breach, breach of the security of the system, or any similar incident defined under Applicable Law for which notification to a Controller is required under Applicable Law.

"**Products and Services**" means the Company's commercially available products and services that Customer has purchased either directly from Company or through one of Company's authorized channel partners.

"**Transfer**" or "**Transferred**" means the transfer or disclosure or any other type of access to Personal Data to a person, organization or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

2. PURPOSE & CUSTOMER INSTRUCTIONS

2.1 With respect to any Personal Data processed under the Agreement, You shall be the "Controller" and/or the "Business"; We shall be the "Processor" and/or "Service Provider." Company will only collect, use, disclose, or otherwise Process Personal Data for the purposes of performing and/or providing Company Products and Services, in connection with detecting and responding to data security incidents and protecting against fraudulent or illegal activity, and as otherwise permitted or required under the Agreement (including this DPA).

Customer hereby instructs Company to Process Personal Data for the aforementioned purposes, including Transfers of Personal Data to any country in connection with carrying out such purposes. We will not Process Personal Data for any other purpose, and We will not sell Personal Data as the term "sell" is defined under Applicable Law.

2.2 Our Processing shall be done in accordance with Your written instructions, which are finally and completely reflected under this DPA. Unless prohibited by Applicable Law,

we will inform You if (a) Your instructions conflict with Applicable Law, or (b) Applicable Law requires Processing contrary to Your instructions.

2.3 The subject-matter and duration of the Processing, the nature of the Processing, the type of Personal Data and categories of Data Subjects are set out in *Exhibit A* of this DPA.

2.4 You are responsible for ensuring You have a valid legal basis for the Processing contemplated hereunder, and that any required Data Subject consent is duly provided and documented, and You represent and warrant that You have complied with all Applicable Laws in collecting, providing, and/or making Personal Data available to Us such that We are entitled to Process Personal Data in accordance with the Agreement and this DPA. You agree that We shall have no liability arising from the Processing of Personal Data in accordance with Your written instructions. You agree to hold Us harmless and indemnify Us for any damages suffered due to the Processing of Personal Data in accordance with Your instructions.

2.5 In accordance with Applicable Laws, We shall implement technical and organizational measures intended to provide a level of security appropriate to the risks presented by the Processing of Personal Data, consisting of the technical and organizational measures set out in *Exhibit B*. These measures are intended to help protect Personal Data against (a) unauthorized or accidental access or disclosure, and (b) unauthorized or accidental loss or destruction.

2.6 Persons authorized by Us to Process Personal Data are under contractual, professional, statutory, or other binding obligations of confidentiality.

3. REQUESTS TO ACCESS PERSONAL DATA AND REQUESTS FROM SUPERVISORY AUTHORITIES

3.1 If a Data Subject makes a request to Us for access, correction/rectification, deletion/erasure, portability, objection, or any other purported right relating to Personal Data for which We can identify You as the Controller, We will refuse the request, provide the Data Subject with Your contact information, and instruct the Data Subject to direct the request to You.

3.2 If compelled to disclose Personal Data for which You are the Controller due to a request by a law enforcement agency or other third-party, We will give You notice of such request before granting access and/or providing Personal Data, to allow You to seek a protective order or other appropriate remedy. If We are legally prohibited from providing You notice, We will take measures to protect Personal Data from undue disclosure, as if it were Our own Confidential Information being requested.

4. PERSONAL DATA BREACH

We will notify You without undue delay, and within any deadline required by Applicable Laws, after becoming aware of a Personal Data Breach, and will endeavour to take all steps required by law to mitigate the effects of such Personal Data Breach. We shall take commercially reasonable action to assist You in relation to any notifications that You are required to make under Applicable Laws as a result of such Personal Data Breach.

5. TRANSFER

You authorize Us to Transfer Personal Data for the purposes set forth in this DPA. If Personal Data subject to the Applicable Laws of Argentina, the European Economic Area, Switzerland, and/or the United Kingdom is Transferred by You to any Company entity located in a country that has not been found to provide an adequate level of protection under such Applicable Laws, the Parties agree that the Transfer shall be governed by the Data Transfer Addendum, which is incorporated herein by reference.

6. ENGAGEMENT OF SUB-PROCESSORS

6.1 You hereby grant Us a general authorization to appoint Sub-processors (and to permit each Sub-processor appointed in accordance with this Section 6 to appoint Sub-processors). This includes and authorization for Us to engage Our Affiliates to provide some of the Products and Services, and You agree that such Affiliates may access or Process Personal Data to fulfil Our contractual obligations under the Agreement or to provide Products and Services on Our behalf.

6.2 Whether the Sub-processor is a Company Affiliate or a third-party, We will:

a. restrict Sub-processors' access to Personal Data only to what is necessary to maintain or provide the Products and Services to You;

b. impose substantially similar appropriate contractual obligations in writing upon Sub-processors that are no less protective than the obligations set forth in this DPA; and

c. remain responsible for Sub-processors' compliance with and performance of the obligations of this DPA.

6.4 The list of Our Sub-processors, including Affiliates, is available on the Trellix Legal Notices web page (https://www.trellix.com/en-us/assets/docs/legal/enterprise-sub-processor-list.pdf). To be notified of new or changes in Sub-processors, You must register for notifications available here. We will provide notification of new or changes to Our Sub-processor(s) via such e-notifications before authorizing any new or replacement Sub-processor(s) to Process Personal Data in connection with the provision of the Products and Services at least ten (10) days in advance of such change. Where You are required to do so by Applicable Laws, You may object to the engagement of any new Sub-processor within ten (10) days following Our notice regarding such Sub-processor. Your objection must be in writing and provide commercially reasonably justification for the objection, based on reasonable concerns concerning the proposed Sub-processor's practices relating to data protection. Following any objection, Customer and Company will work in good faith to address Customer's objection; if Customer's written concerns cannot be resolved within ninety (90) days, Customer may terminate the Agreement in respect of the applicable Product(s) or Service(s) in relation to which the Sub-processor will Process Personal Data.

7. AUDIT

7.1 Subject to relevant confidentiality obligations, We agree, upon Your request and up to once per year, to:

a. provide copies of documentation designed to enable You to verify Our compliance with the technical and organizational measures set forth in *Exhibit A* to this DPA; and

b. provide written responses, on a confidential basis, to reasonable requests for information made by You, including responses to information security and audit questionnaires, which are reasonably required to confirm Our compliance with this DPA and the GDPR.

7.2 In addition to the foregoing, solely to the extent required by Applicable Laws or a binding request by a regulatory body, You may perform an audit of the Products and Services that Process Personal Data. If a third-party is to conduct the audit, the third-party must not be a competitor to Trellix, and such third-party is subject to our prior assent, and must execute a written confidentiality agreement with the Parties before conducting the audit.

7.3 To request an audit, You must submit a detailed audit plan at least two (2) months in advance of the proposed audit date to Us, which plan describes the proposed scope, duration, and start date of the audit. We will review the audit plan and provide You with any concerns or questions (for example, any request for information that could compromise the Company's security, privacy, employment, or other relevant policies; or any concerns or questions about the proposed third-party auditor). Both Parties will work cooperatively in good faith to agree on a final audit plan. If the requested audit scope is addressed in a similar audit report within the prior twelve months and We confirm there are no material changes in the controls audited, You agree to accept those findings in lieu of requesting an audit of the controls covered by the report.

7.4 The audit must be conducted during regular business hours at the applicable facility and may not interfere with business activities or with Our confidentiality obligations to other customers.

7.5 You will provide Us with any audit reports generated in connection with any audit under this section, unless prohibited by Applicable Law. You may use the audit reports only for the purposes of meeting the requirement of Applicable Law and/or the binding request by a regulatory body that gave rise to the audit. The audit reports and any other materials, documents, communications, and/or information relating to the audit are Confidential Information of the Parties under the terms of the Agreement.

7.6 Any audits are at Your expense. Any request for Us to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from, or in addition to, those required for the provision of the Products and Services. We will seek Your written approval to pay any applicable fees before performing such audit assistance.

8. DELETION OF PERSONAL DATA

Upon expiration or termination of the Agreement, We shall, upon Your request, delete Customer's Personal Data in accordance with the standard functionality of the service, in a standardized format. Company (including its Affiliates) may retain Personal Data to the extent required by applicable laws and the Agreement and will apply the protections of this DPA to Personal Data until such time as it is deleted.

9. ASSISTANCE

9.1 Subject to the nature of the processing and the information available to Us, We will provide You, upon written request, with commercially reasonable assistance in (a) the fulfilment of Your obligation to respond to Data Subjects' requests for exercising data protection rights under Applicable Law, and (b) Your compliance with the obligations pursuant to Article 32 through 36 of the GDPR.

10. MISCELLANEOUS

10.1 Notwithstanding anything to the contrary, the Parties acknowledge that the Applicable Laws are not intended to jeopardize or undermine the confidentiality obligations to which the Parties are subject to in the Agreement or an agreed upon written non-disclosure agreement.

10.2 This DPA shall remain effective as long such Agreement remains in full force and effect. Any terms of this DPA which by their nature should survive termination of this DPA shall survive such termination.

10.3 In the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail regarding the Parties' data protection obligations relating to Personal Data. In cases of doubt, this DPA shall prevail where it cannot be clearly established whether a clause relates to a Party's data protection obligations.

10.4 Should any provision or condition of this DPA be held or declared invalid, unlawful, or unenforceable by a competent authority or court, then the remainder of this DPA shall remain valid.

10.5 Instructions, notices and other communications made under this DPA shall be made in accordance with the Notice provisions of the Agreement.

10.6 Any amendments to this DPA shall be in writing duly signed by authorised representatives of the Parties.

EXHIBIT A
DESCRIPTION OF THE PROCESSING OF CUSTOMER PERSONAL DATA

Subject Matter, Nature, and Duration of the Processing. The nature and subject matter of the Processing are set forth in the Agreement. The Processing will continue for so long as the Agreement remains in effect between the Parties.

Purposes for which Personal Data is Processed. See Section 2.1 of this DPA.

Categories of Data Subjects whose Personal Data is Processed. Customer's end users of Products and Services, including Customer's employees, contractors, contingent workers, business partners, vendors and any other end users that receive access to the Products and Services through Customer.

Categories of Personal Data Processed. Details about Customer end users' computers, devices, applications, and networks, including internet protocol (IP) address, cookie identifiers, mobile carrier, Bluetooth device IDs, mobile device ID, mobile advertising identifiers, MAC address, IMEI, Advertiser IDs, and other device identifiers that are automatically assigned to computers or devices of Customer end users when accessing the Internet, Browser type and language, language preferences, battery level, on/off status, geo-location information, hardware type, operating system, Internet service provider, pages that Customer end users visit before and after using the Products and Services, the date and time of site visits, the amount of time end users spend on each page, information about the links you click and pages viewed within the Products and Services, and other actions taken through use of the Products and Services such as preferences.

EXHIBIT B
TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

The Technical and Organizational Security Measures can be found at the following link: https://www.trellix.com/en-us/about/legal.html

-End-