



**IMPORTANT: READ CAREFULLY. LICENSE/PURCHASE/USE OF TREND MICRO SOFTWARE AND APPLIANCES BY BUSINESS, GOVERNMENTAL, AND OTHER LEGAL ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND CONDITIONS. A DIFFERENT TREND MICRO AGREEMENT GOVERNS THE LICENSE/PURCHASE/USE OF TREND MICRO PRODUCTS THAT ARE PUBLISHED BY TREND MICRO FOR NON-BUSINESS USE, PERSONAL USE, HOME USE, AND/OR CONSUMER USE.**

**TREND MICRO GLOBAL BUSINESS SOFTWARE AND/OR  
APPLIANCE AGREEMENT**

**Trial and Paid Use:** This Business Software and Appliance Agreement supersedes all prior versions published by Trend Micro with respect to transactions consummated on or after the Publication Date  
**Publication Date:** 1 January 2021  
**Version:** English/Multi-Country

IF COMPANY AND TREND MICRO HAVE ENTERED INTO A MANUAL/ELECTRONIC SIGNATURE-BEARING CORPORATE LICENSE AGREEMENT (OR OTHER SIMILAR DOCUMENT) WITH RESPECT TO THE LICENSE/SALE OF ANY TREND MICRO SOFTWARE, APPLIANCE, OR MAINTENANCE, THEN SUCH AGREEMENT WILL GOVERN AND CONTROL THE POSSESSION/USE OF ANY PRODUCTS LICENSED OR SOLD TO COMPANY THEREUNDER AND THIS AGREEMENT WILL HAVE NO EFFECT WITH RESPECT THERETO. OTHERWISE, THE TERMS AND CONDITIONS OF THIS AGREEMENT SHALL GOVERN AND CONTROL COMPANY'S LICENSE/PURCHASE, POSSESSION, AND USE OF ALL PRODUCTS ACQUIRED HEREUNDER. UNLESS PROHIBITED UNDER MANDATORY APPLICABLE LAW WITHOUT THE POSSIBILITY OF WRITTEN WAIVER, IF COMPANY IS PRESENTED A VERSION OF TREND MICRO'S TERMS AND CONDITIONS OF AGREEMENT (SUCH AS "SHRINK-WRAP" OR "CLICK-WRAP" EULA OR SIMILAR DOCUMENT) THAT IS DATED (EITHER EFFECTIVE DATE OR PUBLISHED DATE) PRIOR TO THE PUBLICATION DATE HEREOF (EACH A "PRIOR VERSION") THAT MAY APPEAR AND REQUIRE COMPANY'S ACCEPTANCE DURING THE REGISTRATION/INSTALLATION/DEPLOYMENT OF SUCH PRODUCT, THEN COMPANY AGREES THAT ITS ACCEPTANCE OF SUCH PRIOR VERSION SHALL BE DEEMED TO BE ACCEPTANCE OF THIS AGREEMENT FOR ALL PURPOSES AND SUCH PRIOR VERSION WILL BE MERGED INTO AND SUPERSEDED BY THIS AGREEMENT. Any additional, conflicting, or different terms or conditions proposed by Company in any Company-issued document (such as an Order), are hereby rejected by Trend Micro and excluded herefrom.

**1. Entire Agreement; Not a Master Purchase Agreement; Agreed Definitions.**

**1.1 Entire Agreement.** This Agreement is binding on Company and Trend Micro when referenced or incorporated in a Quote from Trend Micro or a Reseller that directs Company to the website at which this Agreement is posted and Company places an Order for Products in response to such Quote that is accepted by Trend Micro by issuance of a License Certificate to Company for the Ordered Products. If no such Quote is provided to Company but nevertheless Company places an Order for Products with Trend Micro or a Reseller, the Parties agree that such Order, if accepted by Trend Micro by issuance of a License Certificate to Company for the Ordered Products, is licensed/sold on the terms and subject to the conditions set forth in this Agreement (including all policies, procedures, and websites referenced herein) and the issued License Certificate that is incorporated herein by reference and made a part of this Agreement for all purposes. The Parties agree that this Agreement (including the Standard Contractual Clauses and Data Processing Addendum that form a part hereof and set forth certain of the responsibilities of the Parties with respect to GDPR Data) is the final, complete, and exclusive statement of the agreement of the Parties with respect to the subject matter hereof, and any prior written agreements; representations, statements, or advertising of Trend Micro whether oral or written; course of dealing between the Parties or usage of the trade; Orders; or descriptions that are not specifically set forth in this Agreement with respect to the subject matter hereof, are all merged into and superseded by this Agreement. In entering into this Agreement, each Party represents and warrants to the other Party that it is NOT relying on any extrinsic representation, warranty, covenant, promise, forbearance, or inducement of any kind or nature that is or was made by any person that is not specifically set forth in this Agreement. By downloading, installing, deploying, and/or using any Trend Micro Product obtained by Company for which a Trend Micro License Certificate is issued by Trend Micro to Company, Company ratifies and confirms its agreement to this Agreement (including the Standard Contractual Clauses, Data Processing Addendum, and the License Certificate) as the sole and exclusive terms, conditions, limitations, and exclusions governing the purchase/license of such Products. **Direct questions, legal notices, and concerns regarding this Agreement to:** [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)

**1.2 Not a Master Purchase Agreement.** Company acknowledges that this is NOT a master purchase agreement for subsequent purchases of Products, but rather, this Agreement only applies to each instant purchase/license of Products by Company. Each subsequent procurement/license of Products by Company will be made subject to and conditioned on the agreement of the Parties to this Agreement unless otherwise agreed in a writing signed by the Parties.

**1.3 Procurement Under This Agreement.** Company may secure Products under this Agreement by one of three methods:

a. **Procurement Through a Reseller.** Typically, Company will secure a Quote for Products from a Reseller of Trend Micro Products. Based on such Quote, Orders by Company will be sent to the Reseller at such prices, discounts, and on invoice and payment terms as agreed solely by Company and its Reseller. Company understands that if an Order is placed with a Reseller, the Reseller can place an order with Trend Micro for Products (either directly through Trend Micro or through a Trend Micro distributor) as requested by Company. Except for the matters agreed in the first sentence of this paragraph between the Reseller and Company, all other rights, obligations, terms, conditions, limitations, and exclusions regarding Products that are Ordered by Company are exclusively set forth in this Agreement. All payments by Company for Products will be made directly to the Reseller and never to Trend Micro. Company acknowledges that each Reseller is an independent contractor and in no event or circumstance will any Reseller now or hereafter be deemed a joint venturer, partner, fiduciary, or agent of Trend Micro and NO Reseller has been or will be authorized or permitted to have a right to create any binding obligation, responsibility, duty, liability, warranty, guaranty, or any otherwise contract for or act on behalf of Trend Micro or waive or renounce any right of Trend Micro or modify any right, obligation, or agreement of Company set forth in this Agreement.

b. **Direct Purchase from Trend Micro.** Company may (if permitted by Trend Micro) secure a Quote directly from, and place an Order directly with, Trend Micro based on such Quote, which Order if accepted by Trend Micro will be governed solely by the terms, conditions, limitations, and exclusions set forth in this Agreement (including the License Certificate). All prices and payment terms will be as set forth in the Quote and all payments for Products will be made by Company directly to Trend Micro in accordance with the GSA Schedule Pricelist.

c. Procurement on a Store. Company may purchase a right to access and use (in accordance with Section 2.1(b)) certain Products sold on and hosted by an Online Store Provider. In each such instance, Product is sold by such Online Store Provider at prices determined by Trend Micro on payment terms determined by the Online Store Provider, but such Products will be subject to and governed by this Agreement with such other requirements as such Online Store Provider may impose in connection with Company's use of its Store and its services.

**14 Agreed Definitions.** In addition to initially capitalized definitions, descriptions, clarifications, and agreements that may be set forth elsewhere in this Agreement (that include all policies, procedures, and Trend Micro websites made a part hereof) that are referenced/incorporated herein, the initially capitalized definitions, descriptions, clarifications, and agreements shall have the meanings set forth in this Section 1.4 (each is an "Agreed Definition") and all Agreed Definitions shall be equally applicable to the singular, plural, and derivative forms.

"Affiliate" means as to a Party, each person that is Controlled by a Party, that Controls such Party, or that is under common Control with such Party. "Control" means the direct or indirect ownership of more than fifty percent (50%) of the equity shares or interests (or the maximum equity ownership permitted by Applicable Law if such Party is not permitted to own more than 50%) entitled to vote for the directors or other management of such Party or the equivalent, but only for as long as such ownership relationship continues to exist. Upon request, each Party agrees to confirm in writing to the other Party, the status of any or all Affiliates.

"Appliance" means a hardware-based appliance designed and provided by Trend Micro as a Product that inseparably combines Hardware and Integrated Software to form a single purpose, unified device that provides capabilities, features, and functionalities as set forth in its Documentation. The Hardware portion of an Appliance may be sold, leased, rented, or loaned hereunder, whereas the Integrated Software portion of an Appliance is only licensed and never sold.

"Appliance Differing Terms" shall have the meaning set forth in Section 4.

"Applicable Laws" means all mandatory national, federal, provincial, state, municipal, and local laws, statutes, acts, ordinances, regulations, rules, codes, treaties, executive orders, supervisory requirements, official directives, circulars, opinions, interpretive letters, and other official releases in the Territory that are applicable from time-to-time to a Party's performance of its obligations and/or exercise of its rights hereunder, including, without limitation, data protection/privacy laws; corrupt activities/illegal payment laws; economic/trade sanctions rules and regulations; and export/import laws.

"Communications" shall have the meaning set forth in Section 9.

"Company" is the corporation, company, or other legal entity (either public or private) that is listed on the License Certificate for such Products as being the licensee/purchaser. In the event of conflict between an Order and a License Certificate, the License Certificate shall control.

"Company Data" means any data and information that is: (a) automatically forwarded to Trend Micro-owned or -controlled servers by Company's use of any licensed Software or other Products; or (b) otherwise intentionally provided by Company to Trend Micro.

"Company's Configuration" shall have the meaning set forth in Section 2.7.

"Computer" means a Virtual Machine or physical device that accepts information in digital or similar form and manipulates it for a specific result based on a sequence of instructions, including without limitation mainframes, Servers, workstations, desktop computers, laptops, tablets, mobile devices, telecommunication devices, Internet-connected devices, and hardware products capable of operating a wide variety of productivity, entertainment, business, security, and/or other software applications.

"Confidential Information" shall have the meaning set forth in Section 10.

"Contractor" is an independent contractor that provides services in support of Company and/or its Affiliates with respect to any Products provided hereunder pursuant to a written agreement between such Contractor and Company that imposes an obligation (among other obligations) on such Contractor to fully comply with this Agreement to the extent of access to, possession of, and/or use of any Product by such Contractor.

"Controlled Technology" shall have the meaning set forth in Section 17.

"Data Processing Addendum" or "Addendum" means Trend Micro's Data Processing Addendum (at [http://www.trendmicro.com/en\\_us/about/legal-policy/data-processing-addendum](http://www.trendmicro.com/en_us/about/legal-policy/data-processing-addendum) and attached hereto or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)) that is applicable if and to the extent Trend Micro acts as a 'processor' or 'sub-processor' (as defined in the GDPR) for Company of GDPR Data. The Parties agree that the Data Processing Addendum is incorporated herein and made a part hereof for all purposes on the terms and subject to the conditions and limitations set forth herein and therein.

"Delivery Date," "Delivered," and "Delivery." The Delivery Date shall be: (a) for Software, it is the date that Software is made available by Trend Micro for electronic download by Company, and/or (b) for Hardware, the date of actual shipment to Company, but some Appliances may be subject to different delivery terms as notified by Trend Micro. All Products and Maintenance will be deemed for all purposes to be Delivered in the country of Trend Micro's place of business stated in the License Certificate.

"Different Terms" shall have the meaning set forth in Section 3.

"Documentation" means the printed, electronic, and online technical documentation and operating instructions generally made available by Trend Micro for Products provided for the purpose of supporting Company's Internal Business Use of such Products as authorized in Section 2.1.

"End User" means any individual, entity, or person (directly or indirectly through another user) that: (a) accesses or uses a Product licensed hereunder for Company's benefit in accordance with this Agreement such as Company's Administrator(s), technical/support resources, or Company's employees/contractors whose access/use is in furtherance of its Internal Business Use; or (b) otherwise accesses or uses such Product.

"GDPR" means the European Union General Data Protection Regulation with mandatory effect May 25, 2018 that is only applicable to Personal Data that is subject to, regulated by, and protected under the GDPR and shall also include additional laws, rules, and regulations now or hereafter promulgated by the European Union, any Member State, or other governmental authority under or supplemental to the GDPR, as the same may be amended, supplemented or replaced from time to time; and 'controller,' 'processor,' and 'data subject' shall have the meanings respectively assigned to them in the GDPR.

"GDPR Data" shall mean 'personal data' (as defined in Art. 4) under the GDPR that is made available or supplied by Company to Trend Micro pursuant to this Agreement, if and only to the extent that the GDPR applies to Trend Micro with respect to its processing of such Personal Data.

"Global Privacy Notice" means Trend Micro's Global Privacy Notice published from time-to-time at [https://www.trendmicro.com/en\\_us/about/legal/privacy-policy-product.html](https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html) and attached hereto or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com).

"Government Agency" shall have the meaning set forth in Section 18.

"Hardware" means the hardware product that Integrated Software is embedded in or preloaded on by Trend Micro and sold as an Appliance and

all Documentation therefor.

**“Instance”** means an image of software on a physical device or Virtual Machine that is created by executing the software’s setup or install procedure or by duplicating an existing Instance, and thereafter, that Instance is “run” by executing one or more of its instructions. Once running, an Instance is running (whether or not instructions continue to be executed) until it is removed from memory.

**“Integrated Software”** means the object code version of any Trend Micro-published/branded applications software that is embedded in or preloaded on Hardware by Trend Micro to form an Appliance. Integrated Software is licensed hereunder (and no right, title, or interest therein is sold) for a Subscription Period that is no longer than the life of the Appliance and is not re-deployable to replacement Hardware except as may be specifically permitted herein.

**“Internal Business Use”** means the internal business access and use of Product licensed hereunder solely by and for the direct benefit of Company specifically in connection with the security, protection, and/or integrity of Company’s systems, networks, devices, documents, emails, and/or other Company Data.

**“IP Claim”** means any suit, cause of action, or other legal proceeding filed/brought against Company by a third party in the courts of law, equity, or otherwise ONLY in the Territory, that asserts that Software licensed hereunder directly infringes any patent, copyright, and/or trademark of such third party.

**“License Certificate”** means an written (electronic or otherwise) acceptance/entitlement confirmation issued by Trend Micro to Company with the license/purchase of Products that confirms to Company the Products purchased by Company, including the applicable Licensed Capacity where applicable. The License Certificate and this Agreement forms the entire agreement between Trend Micro and Company with respect to each Order of Products that is accepted by Trend Micro. Company is advised to retain the License Certificate as proof of its entitlement to such Products.

**“Licensed Capacity”** is defined (includes quantity, licensing metric, and term of license) as and notified in the License Certificate when Standalone Software is licensed hereunder, the number of licenses of each type of Standalone Software that Company purchases from time-to-time and is then-validly licensed to Company under this Agreement, based upon Trend Micro’s licensing measurement for each particular Standalone Software. The applicable licensing metrics/measurements (which may include, without limitation, measurement by Computer/CPU, Virtual Machine, device, node, Instance, Server, and user, as applicable) available to Company for Standalone Software licensed hereunder will be determined by Trend Micro from time-to-time for each Product.

**“Licensing Entity”** shall have the meaning set forth in [Section 23](#).

**“Maintenance”** of Software shall have the meaning and description set forth in [Section 5](#). Any maintenance or support of Hardware shall have the meaning and description set forth in applicable Appliance Differing Terms.

**“Non-Production Environment”** means Company’s use of an Appliance and/or Software exclusively in a laboratory, test, or research environment (and not in Company’s production environment/systems) that does not access or make use of live production data at any time or for any reason.

**“Online Store Provider”** means an entity that hosts an online marketplace or store (each a **“Store”**) that offers for sale: (1) such entity’s infrastructure (IaaS) and/or platform (PaaS) hosting services by separate agreement and a separately-stated service fee with the customer; together with (2) the software applications of third party publishers (such as Trend Micro) that are offered and resold (for a separately-stated royalty/fee) by such service provider entity for deployment on its infrastructure and/or platform, but licensed to the customer by the publisher for a Subscription Period. With respect to the access and use of any Trend Micro Standalone Software that is procured by Company on an Online Store Provider’s store in accordance with [Section 2.1\(b\)](#), the Parties agree that the Online Store Provider is and will be solely responsible to Company for its infrastructure and/or platform hosting services and Trend Micro is solely responsible to Company for the Standalone Software and the Updating thereof. Examples of such Stores are AWS Marketplace, Microsoft Azure, Google Marketplace/Launcher, and VMware Marketplace.

**“Open Source Software”** means: (1) each and every third party software code/component that is licensed/distributed under a license agreement approved by the Open Source Initiative or similar open source or freeware license (and not this Agreement); and (2) is embedded or included in a Product licensed hereunder; including any of the following Open Source Initiative-approved license agreements: (a) GNU’s General Public License (GPL), Lesser/Library GPL (LGPL), and GNU Affero Public License; (b) The Artistic License (i.e., PERL); (c) the Mozilla Public License; (d) the Netscape Public License; (e) the Berkeley software design (BSD license including Free BSD or BSD-style license; (f) the Sun Community Source License (SCSL); (g) an Open Source Foundation License (e.g., CDE and Motif UNIX user interfaces); (h) the Apache Server license; or (i) the MIT License. For the avoidance of doubt, each individual, third party software code/component of Open Source Software has its own copyright and its own license agreement.

**“Optional Features”** means optional (as may be configured, restricted, limited, and/or disabled by Company in creation of Company’s Configuration) capabilities, features, and functionality (such as the Smart Protection Network and/or Web Reputation Services, each as is more fully described in its Documentation) of a Product licensed hereunder that, among other things, collects and forwards certain Company Data (some of which may be Personal Data) for processing that is necessary to permit Trend Micro to, among other things, provide the capabilities, features, and functionality of such Product, including those that are optional, that Company deems necessary or appropriate for its business needs in determining Company’s Configuration.

**“Order”** means a procurement document placed by Company (with a Reseller or Trend Micro, as the case may be) for the procurement of Products to be supplied only in accordance with and subject to the provisions of this Agreement. All Orders are Customer’s irrevocable commitment to purchase and pay for the Products stated in the Order and are subject to direct or indirect (where the Order is placed with a Reseller) acceptance by Trend Micro at its sole discretion, which acceptance occurs and is signified by Trend Micro’s issuance of a License Certificate to Company for such Products or other Trend Micro performance (the **“Order Effective Date”**).

**“Party”** means only each of the persons entering into this Agreement and all other persons such as Affiliates and Contractors of each Party are third parties without rights or benefits hereunder.

**“Personal Data”** means one or more data elements relating to an identified or identifiable natural person that can be used to identify, directly or indirectly, such natural person to the extent such data is regulated, protected, restricted, or controlled under Applicable Laws (such as, for example, the GDPR) for the protection of that natural person’s privacy and related rights.

**“Perpetual Period”** means with respect to a license granted for Standalone Software that extends for an indefinite period of time, subject to earlier termination in accordance herewith. For the avoidance of doubt, Standalone Software that is licensed for a Perpetual Period never includes a payment for, or a right to receive without additional fees or compensation, Maintenance for the entire Perpetual Period.

**“Products”** means and includes Software, Appliances (including Hardware), and Maintenance that is licensed/purchased hereunder, but does NOT include: (a) Trend Micro **“software-as-a-service”** and **“cloud-based”** service offerings; or (b) PSP services or other premium, enhanced, managed, technical, or engineering services or support that may be provided by Trend Micro pursuant to a separate agreement or statement of work for additional compensation. Trend Micro specifically reserves the right from time to time in its discretion and without incurring any liability to Company: to modify the design, specifications, as well as functionality of any Product; and/or end-of-life (in accordance with Trend Micro published policies) such Product

**“Quote(s)”** means one or more documents issued by Trend Micro or its Reseller (as the case may be) to Company specifying the Software, Appliance, and/or Maintenance that Company seeks to obtain, the related pricing, payment terms, and Licensed Capacity and sufficient other information to complete the transaction. Each Quote shall incorporate this Agreement (whether specifically, by reference, or by publication) as the sole basis and governing document for any procurement by Company based on the Quote.

**“Reseller”** means a reseller, system integrator, independent software vendor, VAR, OEM or other channel partner that is authorized by Trend Micro or its distributor to secure orders for the license/sale of Products to end users, including Company.

**“Separate Modules”** means any plug-in or module for Software that Trend Micro determines to be new or a different product/features/functionality that Trend Micro makes generally available to the public by license for new or additional consideration. Separate Modules are not included with Maintenance or Updates to existing Software.

**“Server”** means a computer or device (and deployed software) on a network that provides functionality, management, and/or support for other devices and/or other network resources, such as a web server, file server, a database server, or a print server.

**“Software”** means the object code version of Integrated Software, Standalone Software, and Test Software and includes all Documentation and Updates thereto made available to and purchased by Company. In no event or circumstance will a source code version of any Software be offered, licensed, or otherwise provided hereunder to Company.

**“Software Limited Warranty”** shall have the meaning set forth in [Section 11](#).

**“Standalone Software”** means the object code version of any applications software (and Updates thereto) that is published by and is generally made available for license from Trend Micro hereunder that does not include any Hardware, nor is it licensed by Trend Micro as part of an Appliance. Standalone Software also includes Instances thereof that are licensed for deployment in a Virtual Machine environment.

**“Standard Contractual Clauses”** or **“Clauses”** or sometimes also referred to the “EU Model Clauses” means the Standard Contractual Clauses (processors) published by the European Commission, which Standard Contractual Clauses are attached to the Data Processing Addendum at [http://www.trendmicro.com/en\\_us/about/legal-policy/data-processing-addendum](http://www.trendmicro.com/en_us/about/legal-policy/data-processing-addendum) and attached hereto or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com). The Parties agree that the Standard Contractual Clauses are incorporated herein and made a part hereof for all purposes on the terms and subject to the conditions and limitations set forth herein and in the Data Processing Addendum, and in the event such Clauses are in conflict with anything contained herein or the Addendum, such Clauses shall govern and control. The Parties further agree that if a subsequent replacement version of the Clauses is published by the European Commission, such replacement version will automatically replace the existing Clauses and apply *mutatis mutandis*; *provided, however*, should Trend Micro at any time put in place other measures to ensure that the transfer is in compliance with the GDPR (such as becoming certified under Privacy Shield), the Parties agree that the version of the Clauses then-in-effect between the Parties will automatically terminate and be superseded by such other measures when those measures take effect.

**“Store”** shall have the meaning as set forth within the definition of Online Store Provider above.

**“Subscription Period”** means, only if available from Trend Micro for a specific version of Software, the limited term/increment of time (*i.e.*, not a Perpetual Period) that the Software is licensed for use by Company. Such Subscription Period may be offered by the week, month, or year (not to exceed three (3) years), during which period, the licensee has the right to use the Software (and receive Maintenance without additional cost) in accordance herewith. After expiration of the Subscription Period, a new Subscription Period or Perpetual Period license must be purchased in order to continue the use of the expired Software. *Integrated Software* is always licensed for the limited Subscription Period that expires and terminates at the end of such Subscription Period, unless such license is earlier terminated in accordance with this Agreement such as when the unit of Appliance on which such Software was originally installed is no longer deployed and used in accordance with the Appliance’s Documentation.

**“Term”** shall have the meaning set forth in [Section 22](#).

**“Territory”** means worldwide other than Japan, subject always to and limited by the terms, conditions, waivers, limitations, disclaimers, and exclusions in this Agreement, and present and future Applicable Laws that applies to the Products and/or the performance of either Party hereunder that prohibits or restricts Product sale, use, or access: (a) to certain technology/goods/services; (b) to specified countries; and/or (c) by defined persons.

**“Test Period”** shall have the meaning set forth in [Section 7.1](#).

**“Test Software”** shall have the meaning set forth in [Section 7.1](#).

**“Test Use”** or a **“Test”** shall have the meaning set forth in [Section 7.1](#).

**“Trend Micro”** means in each instance that Products are acquired under this Agreement, the Licensing Entity that provides Products in such instance as determined by application of [Section 23](#).

**“Virtual Machine”** means a software container, implementation, or emulation of a Computer (*i.e.*, a physical device) that runs its own operating system and executes application programs like a physical Computer.

**“Updates”** means and includes if and when generally made available by Trend Micro with respect to Software licensed hereunder that is also subject to then-paid Maintenance, new object code versions (including patches) of such Software that includes: (a) improvement of features/functionality that is used to identify, detect, and block computer viruses, spam, spyware, malicious code, websites, or other forms of computer abuse generally categorized as malware and other forms of content identification or categorization; (b) corrections, modifications, revisions, patches, new definition files, maintenance updates, bug fixes and/or other enhancements to, or for use in connection with, the Software; and/or (c) major or minor new versions of existing Software that contains new features, improvements to existing features, capabilities, structures, and/or functionality that Trend Micro makes available to existing customers that have then-purchased Maintenance for such Software; *provided, however*, the term “Updates” specifically excludes Separate Modules and does not apply to the Hardware component of any Appliance. The access to and use of certain new versions, features, and/or functionality that Trend Micro may offer to make available to Company from time-to-time as an Update may be (at Trend Micro’s determination) subject to and contingent upon Company’s prior agreement to additional terms and conditions that are applicable to such new versions, features, and/or functionality. Updates that are released by Trend Micro from time-to-time replace or patch and will become part of previously licensed copies of the updated Software and will not increase the units/Licensed Capacity of Software licensed hereunder, or otherwise create additional copies or licenses of such Software, nor does any Update create any new or additional warranty for the Software it Updates.

## **2. Software License; Right to Copy; Limitations**

**21 Software License.** Products are protected by patent, copyright, trade secret, and/or other worldwide intellectual property Applicable Laws. On the terms and subject to Company’s continuous compliance with the conditions set forth in this Agreement (including the License Certificate) and on the condition precedent of Company making payment as directed in [Section 1.3](#), Trend Micro hereby grants only to Company solely for the Internal Business Use of Company (and any of its Affiliates and/or Contractors as it permits in accordance with [Section 2.5](#)), a non-exclusive, non-transferable (except as may be required for Standalone Software licenses in the European Union under mandatory Applicable Laws that do not permit a written waiver or limitation), non-assignable (by operation of law or otherwise), and revocable (in accordance herewith) right and license (with no right to sublicense) in the

Territory to: (a) install or have installed (on Computers owned by or under the control of Company through written agreement with a Contractor), access, and use Standalone Software only as permitted in its Documentation, each of the foregoing for the stated Subscription Period (unless the License Certificate states that such Standalone Software is being licensed for a Perpetual Period) and in such Licensed Capacity as is listed in the License Certificate; (b) access and utilize (only as permitted in its Documentation) for a Subscription Period for the Licensed Capacity purchased, Standalone Software licensed hereunder that was purchased on a Store to be hosted (for separate service fee) by that Online Store Provider on its infrastructure/platform under a separate service agreement between Online Store Provider and Company; (c) use Integrated Software (only as permitted in its Documentation) forming a part of any Appliance purchased hereunder only for such limited time (not for a Perpetual Period) as it forms a part of the unit of Appliance that it is originally shipped by Trend Micro to Company; and/or (d) with respect to any Software that offers Trend Micro cloud-hosted functionality and/or Optional Features that have been selected in Company's Configuration, Company may enable, access, and/or utilize such cloud-hosted functionality and/or Optional Features portion (if any) in accordance with applicable Documentation only: (i) during a Subscription Period for Software licensed for that limited term; or (ii) during the first year of newly-Licensed Capacity of such Software licensed for a Perpetual Period and for such time thereafter that Company purchases Maintenance for such Software.

**22 Right to Copy.** With respect to Standalone Software licensed under Section 2.1(a) only, Company shall have the right to reproduce, without additional cost, a commercially reasonable number of copies of the Standalone Software (in an unmodified form) and its Documentation that is licensed to Company only for backup/failover, archive, and/or training purposes, *provided* that Company reproduces on or in such copies any and all of the copyright, trademark, patent, and other proprietary notices or markings that appear on the original copy of the Standalone Software (and Documentation). No copy of Standalone Software will be utilized for production purposes (other than backup/failover testing or archive retrieval) except for such time as the production copy of such Standalone Software is not being utilized for production use.

**23 Limitations/Conditions.** Except as may be specifically granted hereunder by license to Company in this Section 2 or to the extent prohibited by or inconsistent with any Different Terms licensing Open Source Software to Company, Company agrees that it is not licensed hereunder to and as a condition hereunder, will not (or otherwise allow third parties to): (a) modify, adapt, alter, translate, or create derivative works (as defined under Applicable Laws) from any part of any Software (or its Documentation) or authorize others to undertake any of the foregoing prohibited acts; (b) merge or embed any Software with or in other software, sub-routines, or other binary code segments; (c) reverse engineer, reverse compile, decompile, or disassemble any Product or object code thereof, or otherwise attempt to decrypt, decode or discover the source code or underlying ideas or algorithms of any Software or part thereof, including but not limited to sub-routines, functions, libraries or other binary code segments of Software except and only to the minimum extent required to be permitted with respect to interoperability under mandatory Applicable Law without the possibility of waiver; (d) distribute, license, sublicense, lease, sell, rent, loan, mortgage, encumber, auction, or otherwise transfer or provide a copy of any Software (or components thereof including any license or access key or authorization) to any third party; (e) publish, provide, or otherwise make available to any third party, any competitive, performance, or benchmark tests or analysis relating to the Software without the written permission of Trend Micro which may be withheld or conditioned at the sole discretion of Trend Micro; (f) deploy or use Software or Appliance in any manner other than as expressly permitted in its Documentation; (g) permit any third party to use or benefit from the use or functionality of any Product (alone or in combination with any other product or service) via, for instance, third party outsourcing facility or service, service bureau arrangement, time sharing basis, or as part of any other hosted or platform service that permits either access to or use of any Products, whether on a specific fee basis or otherwise; or (h) attempt to do any of the foregoing. Company understands and agrees that all Software and Appliances are subject to End-of-Maintenance/Support policies forming a part Trend Micro's policies referenced in Sections 4 and 5 below.

**24 Use Exclusions.** Products are not fault-tolerant/fail-safe and are not designed, intended, suitable, or licensed hereunder for use, and may not be used, in situations or environments requiring extra safety features or functionality for fail-safe or fault-tolerant performance, such as: (a) the design, construction, operation, or maintenance of any nuclear facility, civil infrastructure such as power plants and waterworks, manufacturing facilities, or industrial plants such as chemical refineries; (b) aircraft navigation, communications, or operating systems; (c) air traffic control systems; (d) operation of life-support or life-critical medical equipment; or (e) any other equipment or systems in which the circumvention, unavailability, inaccuracy, ineffectiveness, or failure of the Product could lead or contribute to death, personal injury, or physical property/environmental damage, and Trend Micro specifically excludes any right or license for any such use and disclaims any express or implied warranty/guarantee of fitness for any such use. Only as may be specifically set forth in the Documentation therefor, Trend Micro notifies Company that no Product has been submitted for compliance testing, certification, or approval for any use by any governmental agency and/or a self-regulatory, standard-setting, or other industry/product-specific consensus organization.

**25 Affiliate and/or Contractor Use; BYOL.**

**251 Affiliate and/or Contractor Use.** For no more than the Licensed Capacity purchased by or on behalf of Company as evidenced in a License Certificate, Trend Micro grants Company the right to authorize and permit (for no additional fees or amounts due Trend Micro other than the fees already payable with respect to licenses purchased by Company): (a) Company's Affiliates to access, deploy, and/or utilize Products only in connection with Affiliate's Internal Business Use for so long as such person remains an Affiliate of Company; and (b) Contractors to Company and/or its Affiliates to access, install, deploy, and/or utilize Products only in connection with the provision of business process support, technical support, or outsourcing services to and solely for the use and benefit of Company and/or Affiliates in connection with its and their Internal Business Use and not for the benefit of any third party or such Contractor, all of the foregoing on the terms and subject to the limitations and conditions of this Agreement. Each Affiliate and Contractor having access to, possession of, and/or utilization of any Product will be considered an authorized user of Company under this Agreement with respect to such Product and NOT a separate or additional licensee or otherwise having any rights or deemed to be a third party beneficiary hereunder in any event or circumstance. Company agrees at all times to require, ensure, and enforce compliance with the grants, terms, conditions, and limitations set forth in this Agreement as well as the Data Processing Addendum and Standard Contractual Clauses where applicable by Company's Affiliates (including, without limitation, those applicable to the Affiliate's GDPR Data that may be exported outside of the EEA to Trend Micro by the Affiliate's use of any Product licensed to Company) and/or Contractors having access to Products procured hereunder and, further, Company agrees that it shall at all times be and remain legally and financially responsible to Trend Micro for the compliance and non-compliance with, or breach of, this Agreement and the Standard the Data Processing Addendum/Contractual Clauses where applicable caused by any Affiliate or Contractor. For the avoidance of doubt, since all Maintenance is to be provided by Trend Micro only to Company, no Affiliate and/or Contractor will be entitled to request or receive Maintenance directly from Trend Micro.

**252 BYOL.** In addition to the rights and obligations of Company in connection with Contractor use in Section 2.5.1, the Parties agree that all or any portion of the Licensed Capacity of Standalone Software licensed for a Perpetual Period (unless otherwise authorized in the applicable Documentation as being available for Products that are licensed for a prepaid Subscription Period) pursuant to Section 2.1(a) that is subject to then-current paid Maintenance may be deployed and hosted on the infrastructure/platform of a Contractor in a Bring-Your-Own-License (BYOL) environment for the sole access, use, and benefit of Company and/or its Affiliates in accordance herewith. In partial consideration for Trend Micro granting the foregoing rights without the payment of additional monies, Company agrees that Trend Micro will have no responsibility to Company in any event or circumstance for, or liability or otherwise subject to or liable for any damages whatsoever to Company with respect to, the actions or inactions of any such Contractor or breach of its agreement with Company.

**26 Ownership; Compliance Tools.** The Parties understand and agree that all Software is licensed and not sold hereunder. The Parties agree that, as between the Parties, all Software and its Documentation, and all worldwide intellectual property rights therein or related thereto, are the exclusive property of Trend Micro, its Affiliates, and/or its or their licensors/suppliers. All rights in and to Software not expressly granted to Company in this Agreement are reserved by Trend Micro and Company will have no other or different rights (implied, by estoppel, or otherwise) or privileges with respect to any Software. Nothing in this Agreement will be deemed to grant, by implication, estoppel, or otherwise, a license under any of Trend Micro's existing or future patents or other intellectual property rights. Trend Micro reserves the right to take any and all reasonable steps to prevent unauthorized access to, and use of, Software by any person. Company acknowledges and agrees that Trend Micro may utilize and deploy in connection with any or all Products: (a)

registration or license keys or authorization codes that are required for activation and/or renewal of each or all copies or use of a Product; and/or (b) other compliance tools, processes, procedures, and/or controls to ensure that Company has purchased full entitlement for Products it has deployed.

## **27 Use of Company Data.**

**27.1 Company Data Provided to Trend Micro; GDPR Data.** Company understands and agrees that the installation and/or use of each Product and the Maintenance thereof will require that Company provide or make available Company Data (including any GDPR Data and/or Personal Data) to Trend Micro. Company may: (a) as and to the extent stated or permitted in the applicable Documentation for a specific Product, elect to set the Company Configuration (as discussed further in Section 2.7.2) of a Product to automatically forward (without human command or intervention) certain Company Data (including any GDPR Data and/or Personal Data) to Trend Micro-hosted or -controlled servers (for example, by enabling certain Optional Features of a Product); and/or (b) intentionally provide certain Company Data (which may also be GDPR Data and/or Personal Data) to Trend Micro in connection with (i) Product registration, activation and/or deployment/redeployment of a Product, and/or (ii) Maintenance provided by Trend Micro to Company in relation to such Product. Company authorizes Trend Micro to utilize Company Data (that may also be GDPR Data and/or Personal Data) for the effective delivery of the features, functionality, and benefits of Trend Micro's Products, Maintenance, and other services to Company as well as to further its understanding of, and improve, the usability, capabilities, and effectiveness of Trend Micro's Products, Maintenance, and other services for Company and other customers and business partners of Trend Micro. For information on how Trend Micro utilizes Personal Data comprised in Company Data, please see the Global Privacy Notice.

By entering into this Agreement, each of Company and Trend Micro acknowledges and agrees that it is also entering into and agreeing to be bound by the attached: (1) the Data Processing Addendum; and (2) the Standard Contractual Clauses, it being further agreed that each of the Addendum and Clauses shall only apply, on the terms and subject to the conditions and limitations set forth herein and therein, if and to the extent that Trend Micro acts as a processor or subprocessor for GDPR Data (but not other Company Data) that Company (and its Affiliates that have been authorized to access, deploy, and/or utilize Products pursuant to Section 2.5) provides or makes available to Trend Micro hereunder. If any Affiliates of Company utilize any Products, Company hereby enters into and agrees to be bound by the Data Processing Addendum and the Standard Contractual Clauses for itself and on behalf of each such Affiliate, and Company represents and warrants to Trend Micro that Company is duly authorized, and Company and all such Affiliates have each taken, all necessary action to do so validly.

**27.2 Company's Configuration of Optional Features.** Company acknowledges and agrees that selection (during activation/initial deployment and at all times thereafter) and use of Optional Features in each Product is solely Company's responsibility in connection with the creation of Company's Configuration of each Product and assuring that Company's Configuration conforms to Company's requirements, policies, and procedures regarding any processing of Company Data (including any GDPR Data and/or Personal Data) and complies with all Applicable Laws in each jurisdiction to which Company's processing of any Company Data may be subject (including any GDPR Data and/or Personal Data) and/or from which Company is accessing and utilizing an Optional Feature of such Product. Therefore, Company agrees to: (1) review the capabilities, features, and functionality of the Optional Features in the Documentation thereof; and (2) configure, restrict, limit, and/or disable each Optional Feature in order to cause its Company Data to be utilized in a manner that meets Company's specific needs and Applicable Laws (each Product as configured by or on behalf of Company from time-to-time is herein referred to as "**Company's Configuration**"). Except for Optional Features and permissions and administrative selections described in the Documentation, Company understands that each Product is a standard off-the-shelf software or hardware-based appliance and no additional or different instructions or configurations are available to Company for such Product.

**28 Security Acknowledgement.** Due to the continual development of new techniques for intruding upon and attacking networks, systems, and/or Computers, Trend Micro does not represent, warrant or guarantee: (1) that Products will detect, block, or completely remove, or clean any or all applications, routines, and files that are malicious, fraudulent or that Company does not use or want; or (2) that any Product or any data, equipment, system or network on which a Product is used (or protects) will be free of vulnerability to intrusion or attack. Company agrees that the success of security efforts and the operation and protection of its Computers, networks, and data are dependent on factors solely under Company's control and responsibility, including, but not limited to: (a) the design, implementation, deployment, and use of hardware and software security tools in a coordinated effort to manage security threats; (b) the selection, implementation, and enforcement of appropriate internal security policies, procedures and controls regarding access, security, encryption, use, and transmission of data; (c) development of, and ongoing enforcement of, processes and procedures for the backup and recovery of any system, software, database, and any stored data; and (d) diligently and promptly downloading and installing all Updates to Products made available to Company.

**3. Open Source Software.** The Software may come bundled or otherwise be distributed with Open Source Software that is subject solely to the agreement terms, conditions, limitations, and disclaimers of the specific license (each "**Different Terms**") under which such Open Source Software is redistributed to Company by Trend Micro and NOT this Agreement. Different Terms applicable to any Open Source Software redistributed in any Software provided hereunder will be identified by Trend Micro in the Documentation for, and/or in a "Read Me" or an "About" file in, the Software. OPEN SOURCE SOFTWARE IS PROVIDED BY TREND MICRO "AS IS, WITH ALL FAULTS, AS AVAILABLE" WITHOUT (AND TREND MICRO SPECIFICALLY DISCLAIMS) ANY GUARANTEE, CONDITION, OR WARRANTY (EXPRESS, IMPLIED, OR OTHERWISE) OF ANY KIND OR NATURE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, AND/OR NON-INFRINGEMENT. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS AGREEMENT, AS IT RELATES TO ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH OPEN SOURCE SOFTWARE, TREND MICRO SHALL HAVE NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWSOEVER CAUSED AND/OR OTHERWISE BASED ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF OPEN SOURCE SOFTWARE, EVEN IF TREND MICRO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**4. Appliances.** Several Products available hereunder are Appliances. As such, each Appliance has certain terms and conditions applicable thereto that are in addition to, or different than, those set forth herein (all are "**Appliance Differing Terms**"). In the event Company is licensing/acquiring/leasing/renting/testing/evaluating an Appliance hereunder, Company agrees that the applicable Appliance Differing Terms are incorporated herein by reference and made a part hereof for all purposes. Appliance Differing Terms may include, among other things: a modified and/or different license grant and/or Maintenance for the Integrated Software that forms a part of the Appliance; Hardware warranty and ownership; and/or a description of available maintenance and support for Hardware and the Appliance in general. In the event of conflict between the terms and conditions in the body of this Agreement, and those Appliance Differing Terms, the applicable Appliance Differing Terms shall govern and control. Appliance Differing Terms are set forth at non-materially [https://www.trendmicro.com/en\\_us/about/legal/appliance-differing-terms.html](https://www.trendmicro.com/en_us/about/legal/appliance-differing-terms.html) and attached hereto as may be updated from time-to-time and at any time.

**5. Maintenance.** All Standalone Software licensed for a limited term Subscription Period by Trend Micro includes paid Maintenance in the price of the license for the entire Subscription Period that is purchased by Company. However, Standalone Software licensed for a Perpetual Period hereunder includes Maintenance only for a period of one (1) year from Delivery of the Standalone Software, thereafter, additional Maintenance then-offered by Trend Micro may be purchased for Standalone Software in one (1) year increments. The description of Maintenance and Trend Micro's policies with respect to Standalone Software from time-to-time and at any time are set forth at <https://success.trendmicro.com/support-policies> and attached hereto that are incorporated herein by reference and made a part hereof for all purposes. The description of Maintenance and Trend Micro's policies with respect to Integrated Software are set forth in the Appliance Differing Terms.

**6. Applicable Laws.** To the extent applicable to Company's performance of its obligations and/or exercise of its rights hereunder

(including without limitation in relation to Company's and its Affiliates' (and its and their Contractors') use and/or configuration of any Product), Company represents (on an ongoing basis) and warrants to Trend Micro and agrees that Company and its Affiliates' (and its and their Contractors') will: (1) comply with all Applicable Laws and will not use or configure any Products or give any instructions to Trend Micro which would or could infringe, violate, or otherwise not be in compliance with any Applicable Laws or could cause Trend Micro to do so; and (2) identify, procure, and maintain any permits, certificates, approvals, consents, and inspections that may be required or advisable in order to comply with Applicable Laws with respect hereto. If there is any failure to comply with or breach of this Agreement arising out of or related to this Section, Company will promptly (at no cost Trend Micro) do all things and take all actions as may be necessary or appropriate to cure and correct any breach or non-compliance with any Applicable Laws.

## **7. Test/Evaluation of Appliances and/or Software.**

**7.1 Test/Evaluation.** If Standalone Software or Integrated Software is provided to Company under this Agreement that has been identified by Trend Micro as "Evaluation," "Proof-of-Concept," "Trial," or "Test" Software (each a "**Test Software**"), then the provisions of this Section 7 shall apply thereto and shall supersede any conflicting term or condition of this Agreement. In each of the foregoing instances, Company is granted a royalty-free, non-transferable, limited license to install the Test Software on Computers located in the country of Delivery and owned (unless an Appliance is provided by Trend Micro in connection with Test Use) by Company and only use the Test Software for evaluation of such Test Software in a Non-Production Environment (a "**Test Use**" or a "**Test**") that is limited to thirty (30) days from the date the Test Software is Delivered to Company (or on the date that an Appliance is shipped to Company by Trend Micro for a Test) unless otherwise agreed in writing by Trend Micro (the "**Test Period**"). Sections 2.1, 2.2, and 2.5 of this Agreement do not apply to Test Software, but Sections 2.3, 2.4, and 2.6 do apply to Test Software. If the Test Use involves an Appliance (and Integrated Software), the Parties agree that the applicable Appliance Differing Terms sets forth additional and/or different terms and conditions that are applicable to the Appliance and the Integrated Software that forms a part of that Test Use Appliance. During the Test Period, Company may be able to receive web or email based technical support in the country where Company is located, but otherwise support is not generally available for Test Software or Appliances.

**7.2 Exclusion; Limitation of Liability for Test Software.** TEST SOFTWARE AND ANY APPLIANCE MAY CONTAIN ERRORS OR OTHER PROBLEMS THAT COULD CAUSE SYSTEM OR OTHER FAILURES AND DATA LOSS. CONSEQUENTLY, TEST SOFTWARE IS PROVIDED TO COMPANY "AS IS, WITH ALL FAULTS." TREND MICRO SPECIFICALLY DISCLAIMS AND EXCLUDES ANY WARRANTY, CONDITION, GUARANTEE, AND/OR LIABILITY TO COMPANY OF ANY KIND OR NATURE WITH RESPECT TO TEST SOFTWARE AND ANY APPLIANCE ON WHICH THE TEST SOFTWARE IS DEPLOYED. WHERE LEGAL LIABILITY CANNOT BE EXCLUDED BY THIS DISCLAIMER, BUT MAY BE LIMITED, TREND MICRO'S LIABILITY AND THAT OF ITS SUPPLIERS/LICENSORS/RESELLERS UNDER THIS AGREEMENT RELATED TO TEST SOFTWARE AND ANY APPLIANCE ON WHICH THE TEST SOFTWARE IS DEPLOYED, SHALL BE LIMITED IN THE AGGREGATE TO THE SUM OF FIVE HUNDRED DOLLARS (USD\$500.00) OR THE EQUIVALENT IN LOCAL CURRENCY. Any information about the Test Software gathered from its access or use shall be used solely by Company for the test/evaluation and such information shall not be provided to any third party. Notwithstanding anything contained herein, each Party has the right to terminate any Test Use and the license herein granted at any time with or without reason with five (5) days prior written notice to the other Party. Upon expiration of the Test Period or earlier termination as set forth in this Section 7.2, Company agrees to automatically (and without notice or request from Trend Micro) immediately stop using the Test Software and uninstall, delete, and irretrievably destroy all copies of the Test Software and Documentation including those that may be included in any backup or archive files and shall promptly confirm same to Trend Micro in writing.

**8. Records; Audit.** During the Term and for two (2) years thereafter, Company agrees to retain and make available to Trend Micro accurate and complete records and other system information sufficient to provide verification of the Licensed Capacity of each Product licensed and Company's utilization of Products is and has consistently been in compliance with this Agreement. With at least twenty (20) days prior written notice, and in accordance with Government security requirements, Trend Micro shall have the right to cause an audit (by an internationally-recognized audit firm) to be conducted no more frequently than once each calendar year. If an audit reveals any deployment or use of the Products that is in excess of the Licensed Capacity or is otherwise out of compliance with this Agreement, then Company agrees to promptly correct such non-compliance..

**9. Consent to Electronic and Other Communications and Notices.** Company agrees that Trend Micro may send Company required legal notices and other communications about Products (including Updates), other and/or new Trend Micro products and services, special offers and pricing or other similar information, customer surveys, and other requests for feedback (collectively "**Communications**"). Trend Micro may provide Communications via (among other methods): (a) in-person contacts by Trend Micro and/or Reseller personnel; (b) in-Product notices or email to registered email addresses of named Company contacts; and/or (c) posted Communications on its Websites. With respect to email notices, any such email notice to Company will be sent by Trend Micro to the account administrator(s) named by Company during registration. Company is responsible for ensuring that the email address for the Company's account administrator(s) is accurate and current. Any email notice that Trend Micro sends to the then-current email address will be effective when sent, whether or not Company actually receives the email. By accepting this Agreement, Company consents to receive all Communications through these means.

**10. Confidentiality/Non-Disclosure.** Each Party hereto acknowledges that by reason of its relationship with the other Party hereunder, it may have access to confidential information and materials concerning the other Party's business, technology, and/or products that is confidential to the other Party ("**Confidential Information**"). Each Party's Confidential Information is of substantial value to the Party, which value could be impaired if such information was disclosed to third parties or used in violation of this Agreement. Written or other tangible Confidential Information must at the time of disclosure be identified and labeled as Confidential Information belonging to the disclosing Party. When disclosed orally or visually, Confidential Information must be identified as confidential at the time of the disclosure, with subsequent confirmation in writing within fifteen (15) days after disclosure. Each Party agrees that it will not use in any way for its own account or the account of any third party, such Confidential Information, except as authorized under this Agreement, and will protect Confidential Information at least to the same extent as it protects its own Confidential Information and to the same extent that a reasonable person would protect such Confidential Information. Neither Party may use the other Party's Confidential Information except to perform its duties or exercise its rights under this Agreement. The Confidential Information restrictions will not apply to Confidential Information that is (a) already known to the receiving Party at the time of access hereunder; (b) is or becomes publicly available through no wrongful act of the receiving Party, (c) independently developed by the receiving Party without benefit of the disclosing Party's Confidential Information; (d) has been rightfully received from a third party not under obligation of confidentiality; (e) disclosed in any legal proceeding arising from or in connection with this Agreement; or (f) required to be disclosed by law, provided the Party compelled to disclose the Confidential Information provides the Party owning the Confidential Information with prior written notice of disclosure (only if legally permissible) adequate for the owning Party to take reasonable action to prevent such disclosure. Unless otherwise agreed to by both Parties, upon termination of this Agreement or an applicable Addendum, each Party will return the other Party's Confidential Information. Trend Micro recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor. **In the event that the Parties hereto have previously entered into a non-disclosure or confidentiality agreement that is still in effect on the Order Effective Date of this Agreement, then the Parties hereto agree that such prior agreement is hereby merged into and superseded by this Agreement ONLY with respect to the subject matter hereof and the transactions undertaken pursuant hereto.**

## **11. Limited Warranty – Software.**

**11.1 Limited Warranty.** Trend Micro warrants to Company only that on the initial Delivery Date of any Software licensed under this Agreement and for thirty (30) days after the Delivery Date therefor, that such Software when installed on compliant/compatible hardware and only as permitted in and in accordance with its Documentation, will substantially conform to its Documentation (the “**Software Limited Warranty**”). Any replacement of non-conforming Software will be warranted for the remainder of its original Software Limited Warranty period. In the event that any Software does not comply with the foregoing warranty and such non-compliance is notified to Trend Micro within the warranty period, and if Trend Micro is unable to bring any Software into conformity with the Software Limited Warranty after using commercially reasonable efforts, either Company or Trend Micro may (at the discretion of each) immediately terminate this Agreement for convenience (by giving written notice no later than ten (10) days after the end of the Software Limited Warranty Period) only as to the non-conforming Software. In the event the license is terminated as aforesaid, the license granted to Company to such Software shall immediately terminate. Upon receipt of Company’s certification that it has irretrievably destroyed such terminated Software, Trend Micro shall refund to Company all fees paid by Company for the affected Software. The applicable limited warranty provided by Trend Micro with respect to Integrated Software forming a part of an Appliance is available as directed in Section 4.

**11.2 Warranty Exclusions.** The Software Limited Warranty provided in this Section 11 does not apply to and shall be void: (a) in the event of failure of any Software arising or resulting from improper installation or any modification, alteration, or addition thereto, or any problem or error in the operating system software with which the Software is installed and is designed to operate; (b) if any problem or error in the Software has resulted from improper use, misapplication or misconfiguration, or the use of the Software with other programs or services that have similar functions or features which are incompatible with the Software; (c) if the Software is licensed as Test Software for which Trend Micro does not charge a royalty or license fee; or (d) if Trend Micro does not receive notice of a non-conformity within the applicable warranty period.

**11.3 Exclusive Remedy.** The Parties agree that the rights, obligations, and remedies of the Parties in this Section 11 are in lieu and satisfaction of any right of acceptance/rejection of any Software that Company may have under Applicable Law and Company hereby waives and renounces any right of acceptance/rejection of all Software, it being understood that Company is relying upon its rights under this Section 11. The Parties agree that the warranties and remedies with respect to Software and Maintenance set forth in this Section 11 shall constitute Trend Micro’s sole and exclusive obligation and liability and Company’s sole and exclusive right and remedy for the breach of or Software non-conformance with the Software Limited Warranty herein granted for any Software. COMPANY UNDERSTANDS AND AGREES THAT TREND MICRO CANNOT, AND DOES NOT HEREIN, PROVIDE ANY WARRANTY, GUARANTEE, CONDITION, OR ASSURANCE THAT THE DEPLOYMENT/USE OF ANY SOFTWARE (EITHER BY ITSELF OR IN COMBINATION WITH OTHER TREND MICRO PRODUCTS) WILL GUARANTEE/ASSURE COMPLETE/PERFECT PROTECTION FROM AND AGAINST ALL PRESENT AND FUTURE SECURITY THREATS TO COMPANY’S NETWORKS, SYSTEMS, DEVICES, AND/OR DATA AND NOTHING HEREIN THIS AGREEMENT SHALL BE DEEMED TO IMPLY SUCH A WARRANTY, GUARANTEE, CONDITION, OR ASSURANCE.

**11.4 Disclaimer of All Other Conditions, Guarantees, and Warranties.** EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 11, COMPANY AGREES THAT TREND MICRO PROVIDES SOFTWARE “AS AVAILABLE” AND “AS IS, WITH ALL FAULTS” AND WITHOUT ANY OTHER WARRANTY, CONDITION, UNDERTAKING, OR GUARANTEE OF ANY KIND. TREND MICRO (ON BEHALF OF ITSELF AND ITS SUPPLIERS (BOTH HARDWARE AND SOFTWARE)/LICENSORS/RESELLERS) EXPRESSLY DISCLAIMS ANY GUARANTEES, CONDITIONS AND WARRANTIES (WHETHER STATUTORY, EXPRESS OR IMPLIED) ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE IN TRADE, OR OTHERWISE INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF: MERCHANTABILITY; FITNESS FOR A PARTICULAR OR GENERAL PURPOSE; TITLE; SATISFACTORY QUALITY; NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS; ABILITY TO ACHIEVE A PARTICULAR RESULT; OR OTHERWISE ARISING FROM A STATUTE, CODE, CUSTOM, USAGE OR TRADE PRACTICE, COURSE OF DEALING OR PERFORMANCE, OR THE PARTIES’ CONDUCT OR COMMUNICATIONS WITH ONE ANOTHER; OR ANY WARRANTY AGAINST INTERFERENCE WITH COMPANY’S QUIET ENJOYMENT OF ANY SOFTWARE. COMPANY UNDERSTANDS AND AGREES THAT TREND MICRO DOES NOT WARRANT OR GUARANTEE THAT: (a) SOFTWARE WILL BE CONTINUOUSLY AVAILABLE OR USE THEREOF UNINTERRUPTED; (b) THE FUNCTIONS AND FEATURES CONTAINED IN SOFTWARE WILL MEET THE REQUIREMENTS OF COMPANY OR THAT SOFTWARE WILL SATISFY ANY PARTICULAR BUSINESS, TECHNOLOGICAL, SERVICE, SECURITY, OR OTHER NEEDS OR REQUIREMENTS OF COMPANY; (c) SOFTWARE, UPDATES THERETO, OR MAINTENANCE THEREOF ARE FREE OF DEFECTS, PROBLEMS, BUGS, AND ERRORS OR THAT ALL DEFECTS, PROBLEMS, BUGS OR ERRORS WILL BE DETECTED OR CORRECTED; (d) SOFTWARE WILL DETECT ONLY, ANY, OR ALL SECURITY OR MALICIOUS CODE THREATS; OR (e) USE OF SOFTWARE AND UPDATES WILL KEEP COMPANY’S NETWORKS OR COMPUTER SYSTEMS AND DEVICES FREE FROM ALL VIRUSES OR OTHER MALICIOUS/UNWANTED CONTENT OR SAFE FROM INTRUSIONS OR OTHER SECURITY ATTACKS/BREACHES.

## **12. Exclusions from and Limitation of Liability; Maximum Liability.**

**12.1 Exclusions from Liability.** IN NO EVENT OR CIRCUMSTANCE AND UNDER NO LEGAL THEORY, WHETHER IN TORT (INCLUDING NEGLIGENCE), CONTRACT, UNDER ANY CIVIL CODE, AND/OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL TREND MICRO, ITS AFFILIATES, OR ITS OR THEIR SUPPLIERS (BOTH HARDWARE AND SOFTWARE)/LICENSORS/RESELLERS, BE LIABLE TO COMPANY OR ITS AFFILIATES OR CONTRACTORS UNDER THIS AGREEMENT OR IN CONNECTION WITH ITS SUBJECT MATTER FOR ANY CLAIMS, CAUSES OF ACTION, EXPENSES, LOSSES, OR DAMAGES ARISING FROM OR RELATED TO: LOSS OF USE OF ANY NETWORKS, SYSTEMS, SOFTWARE, HARDWARE, COMPUTERS, OR DEVICES; COMPROMISE, LOSS, OR CORRUPTION OF DATA; LOST OR ANTICIPATED BUSINESS REVENUE; FAILURE TO REALIZE EXPECTED SAVINGS; ANY THIRD PARTY CLAIM AGAINST COMPANY; REDUCTION IN REPUTATION, OR GOODWILL; PROCUREMENT OF SUBSTITUTE GOODS, SOFTWARE OR SERVICES; LOSS OF BUSINESS OPPORTUNITY OR ANTICIPATED SAVINGS; OR OTHERWISE FOR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING FROM OR RELATING TO THIS AGREEMENT, TREND MICRO’S (OR ITS AFFILIATES) PERFORMANCE UNDER THIS AGREEMENT, OR ANY PRODUCT, UPDATES, AND/OR MAINTENANCE, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THIS AGREEMENT FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF TREND MICRO AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR’S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

IF COMPANY IS IN THE EUROPEAN ECONOMIC AREA, REFERENCES TO “INCIDENTAL, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES” SHALL ALSO MEAN ANY LOSSES OR DAMAGES WHICH: (a) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES; (b) WERE KNOWN TO COMPANY BUT NOT TO TREND MICRO; AND/OR (c) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY COMPANY SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO COMPANY DATA.

**12.2 Maximum Liability – Direct Damages.** WITH RESPECT TO THIS AGREEMENT AND THE SUBJECT MATTER HEREOF OR TREND MICRO’S PERFORMANCE HEREUNDER, IN NO EVENT OR CIRCUMSTANCE AND UNDER NO LEGAL THEORY, WHETHER BASED ON CONTRACT; EXPRESS OR IMPLIED OR STATUTORY WARRANTY, CONDITION OR GUARANTEE; MISREPRESENTATION; TORT (INCLUDING NEGLIGENCE); UNDER ANY CIVIL CODE; AND/OR ANY OTHER OR EQUITABLE THEORY LEGAL THEORY, WILL TREND MICRO’S LIABILITY TO COMPANY FOR ACTUAL DIRECT DAMAGES EXCEED IN THE AGGREGATE FOR ALL CLAIMS (AND NOT

PER INCIDENT OR PER CLAIMANT) AND/OR CAUSES OF ACTION UNDER THIS AGREEMENT, THE TOTAL AMOUNT OF LICENSE FEES AND OTHER AMOUNTS PAID OR PAYABLE BY COMPANY FOR THE PRODUCT GIVING RISE TO SUCH CLAIM DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT OR CIRCUMSTANCE FIRST GIVING RISE TO A CLAIM.

**123 Exceptions; Unenforceability.** NOTWITHSTANDING ANYTHING CONTAINED IN THIS SECTION 12 TO THE CONTRARY, TREND MICRO'S LIABILITY SHALL NOT BE LIMITED UNDER THIS SECTION 12 IN THE EVENT OR CIRCUMSTANCE OF: (a) PERSONAL INJURY OR DEATH DIRECTLY ATTRIBUTABLE TO TREND MICRO'S NEGLIGENCE; (b) EVENTS OR CIRCUMSTANCES ARISING FROM THE INTENTIONAL, WILLFUL, OR FRAUDULENT ACTS OF TREND MICRO; (c) BREACH OF TREND MICRO'S CONFIDENTIALITY OBLIGATIONS UNDER SECTION 10; OR (d) PAYMENT OF MONIES BY TREND MICRO UNDER ANY INDEMNITY AGREED HEREIN. THE DISCLAIMERS, LIMITATIONS, AND EXCLUSIONS CONTAINED HEREIN THIS SECTION 12 SHALL APPLY TO THE MAXIMUM EXTENT PERMISSIBLE BY WRITTEN WAIVER, DISCLAIMER, LIMITATION, AND/OR EXCLUSION UNDER THE GOVERNING LAW, REGARDLESS OF WHETHER OR NOT TREND MICRO, ITS AFFILIATES, LICENSORS, SUPPLIERS, AND/OR RESELLERS SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE, BUT NOTHING HEREIN THIS SECTION 12 PURPORTS TO LIMIT TREND MICRO, ITS AFFILIATES, LICENSORS, AND/OR SUPPLIERS LIABILITY TO THE EXTENT OR IN A MANNER THAT WOULD BE IMPERMISSIBLE, UNENFORCEABLE OR VOID UNDER THE GOVERNING LAW.

**124 Basis of the Bargain.** Each Party recognizes and agrees that the waivers, warranty limitations, as well as disclaimers and exclusions from and limitations of liability and/or remedies in this Agreement are a material and essential basis of this Agreement; reflect a reasonable allocation of risk between the Parties; are fair, reasonable, and a fundamental part of this agreement; and each has been taken into account and reflected in determining the consideration to be given by each Party under this Agreement and in the decision by each Party to enter into this Agreement. The Parties acknowledge and agree that absent any of such waivers, disclaimers, exclusions, and/or limitations of liability/remedies, the provisions of this Agreement, including the economic terms, would be substantially different, or in the alternative, this Agreement would not have been consummated.

**13. Intellectual Property Indemnity.**

**131 IP Claim Indemnity.** Trend Micro (at its cost) will have the right to intervene to defend ONLY Company from each IP Claim and indemnify Company from the resulting costs and damages with respect to each such IP Claim finally awarded against Company ONLY that are specifically attributable to such IP Claim or those amounts agreed to by Trend Micro in a monetary settlement of such IP Claim, subject always to the conditions, qualifications and limitations in this Section 13. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. No settlement of any IP Claim will be made by Company (and Trend Micro will have no responsibility or obligation hereunder or otherwise therefor) without Trend Micro's express written consent, which may be withheld at its sole and absolute discretion. The obligation of Trend Micro under this Section 13 for any IP Claim is subject to and conditioned on Company giving Trend Micro: (a) prompt written notice of any IP Claim (but in any event notice in sufficient time for Trend Micro to respond without prejudice to its position), provided that a failure to provide notice shall only relieve Trend Micro of its indemnity obligation to the extent Trend Micro was prejudiced by such failure; (b) sole and complete control and authority over the defense, negotiations, and settlement of such IP Claim; and (c) reasonable requested information, cooperation and assistance, at Trend Micro's expense, with regard to the defense, negotiations, or settlement of such IP Claim. Without Company's consent, Trend Micro will not settle with respect to Company, any IP Claim to the extent such settlement requires that Company admit any liability on the part of Company with respect to such IP Claim or pay any money therefor. Company may participate in the defense of any IP Claim at its cost with counsel of its selection.

**132 Exclusions.** Trend Micro will have no obligation under this Section 13 or otherwise with respect to any IP Claims arising out of, based on, or related to the following: (a) any use of the Software not in accordance with this Agreement or its Documentation; (b) any modification of the Software not made by Trend Micro; (c) Trend Micro's compliance with Company's design, equipment or software requirements, specifications or instructions; (d) any use of any version, revision, or enhancements of the Software by Company other than the most current non-infringing release made available to Company at no charge if such current version would have avoided the IP Claim; (e) any Open Source Software; or (f) any use of the Software in combination with other products, equipment, software, services, data, or technology not specified by the applicable Documentation where the IP Claim would not have arisen or would have been avoided but for such combination.

**133 IP Claim Mitigation.** Should any Software at any time become, or in Trend Micro's opinion be likely to become, the subject of an IP Claim, Trend Micro shall have the right, at its sole option to: (a) procure for Company the right to continue using the Software as licensed hereunder, or (b) modify the Software such that it no longer is the subject of an IP Claim, while maintaining substantially the same functionality of the unmodified Software. If neither (a) or (b) are commercially practicable in Trend Micro's opinion, Trend Micro may terminate this Agreement as to such Software and any related license granted hereunder as to the Software upon written notice, in which event Company will cease further use of the Software and return or uninstall and irrevocably destroy all copies of the subject Software (and Documentation) and, thereafter, Trend Micro will promptly refund to Company, the prorated portion of the license fees paid by Company for the remainder of any unexpired Subscription Period for such Software(s) or, if and to the extent such Software are licensed for a Perpetual Period, Trend Micro shall refund to Company all license fees paid by Company for the affected Software as amortized on a straight line basis over a three (3) year period and any unused, prepaid annual Maintenance fees. The Parties agree that any termination hereof in accordance with this Section 13 shall not be treated as a breach of this Agreement by Trend Micro and shall not entitle Company to any claim for damages, losses, or expenses of any kind or nature arising from or related to such termination including for replacement cost or loss of use of the Software or any lost profits, savings, or revenue arising from or related to the Software. **This Section 13 states Trend Micro's sole and exclusive obligation and liability to Company, and Company's sole and exclusive right and remedy against Trend Micro, for any IP Claim. Except as set forth herein this Section 13, Company acknowledges and agrees that no indemnity is given by Trend Micro with respect to any Software or Appliance and Trend Micro specifically denies and disclaims any obligation to indemnify Company and/or its Affiliates from and against any other matter or thing in any event or circumstance.**

**14. Personal Data.** Company acknowledges that Products licensed hereunder may utilize applications, tools, and procedures to, among other things, receive, collect, transfer, store, and use Company Data (some of which may be GDPR Data and/or Personal Data). Trend Micro has implemented and will maintain commercially reasonable technical, organizational and administrative security measures designed to protect the Personal Data it processes for Company from unauthorized access and misuse while under Trend Micro's custody and/or control. Trend Micro restricts its personnel from processing of Personal Data without proper authorization and imposes appropriate obligations upon its personnel, regarding confidentiality, data protection, and data security of such Personal Data. For additional information on the foregoing, please consult and review the Documentation for each licensed Product, Trend Micro's Global Privacy Notice, and the additional external information therein referenced in the Global Privacy Notice, as well as Section 2.7 that is applicable to Company's Personal Data in most instances.

**15. Assignability.** Subject to limited transfer rights of Standalone Software offered in Section 2.1, Company may not assign all or any portion of this Agreement, whether by contract, operation of law or otherwise, to any person, including any Affiliate, without written approval from Trend Micro, which approval may be withheld or conditioned at the sole discretion of Trend Micro. Any purported assignment by Company shall be void. Trend Micro may assign this Agreement, in whole or part, and delegate its obligations to qualified third parties or Trend Micro Affiliates, provided that no delegation of its obligations shall relieve Trend Micro of its obligations under this Agreement.

**16. Waiver; Severability; Enforcement.**

**161 Waiver.** A Party's failure or delay in enforcing any provision of this Agreement will not operate as a waiver of the right to enforce that provision or any other provision of this Agreement at any time. No waiver of any provision of this Agreement will be valid unless in writing, specifying the provision to be waived, and signed by the Party agreeing to the waiver.

**162 Severability; Enforcement.** The unenforceability of any provision or provisions of this Agreement shall not impair the enforceability of any other part of this Agreement. In the event that any provision of this Agreement conflicts with the governing law under which this

Agreement is to be construed or if any such provision is held invalid or unenforceable in whole or in part by a court with jurisdiction over the Parties, such provision shall be deemed to be restated to the minimum extent necessary to render it valid, enforceable, and insofar as possible, reflect as nearly as possible the original intentions of the Parties. The remaining provisions of this Agreement and the application of the challenged provision to persons or circumstances other than those as to which it is invalid or unenforceable shall not be affected thereby, and each such provision shall be valid and enforceable in accordance herewith.

**17. Export/Import Control.** The export or re-export of Software (and related technical data and services) and/or an Appliance (collectively "**Controlled Technology**") is subject to Applicable Laws with respect to the export (including "deemed export" and "deemed re-export" regulations) and import of Controlled Technology by Company and/or its Affiliates. Company agrees that it will at all times comply with each Applicable Law (now or hereafter in effect) that applies to direct/indirect export, re-export, or import of Controlled Technology by Company and/or its Affiliates and/or the performance of Company and/or its Affiliates hereunder that: (a) requires a license to, or otherwise prohibits the, export, re-export, import, diversion, or disclosure of such Controlled Technology; (b) prohibits or restricts sale, use, or access to certain technology/goods/services, to specified countries, and/or by defined persons; or (c) restricts or prohibits end-use of such Controlled Technology related to the development, production, use, or proliferation of nuclear, chemical or biological weapons, missiles, or other weapons of mass destruction. Company represents and warrants to Trend Micro that neither Company nor any of its Affiliates are under the control of, located in, or a resident or national of any country or region subject to any embargo or applicable trade sanction and are not a prohibited person or entity as defined in any Applicable Law.

**18. Government Agency Use.** All Products (including Software and Appliances) and accompanying Documentation have been developed solely at private expense by Trend Micro and/or its suppliers/licensors/resellers, consisting of commercially-available computer software, commercially-available hardware and appliances, and commercially-available documentation. The acquisition, deployment, duplication, disclosure, and use of Software (as Updated) by any Government Agency may be subject to mandatory Applicable Laws, *however*, except for the limited license granted in Section 2 above to any Software, no right, title, or interest in or to any Software (or Updates and Documentation) is granted or transferred hereunder to any Government Agency licensing such Software. If any Government Agency requires or needs greater or different rights in or to Software other than those rights that are granted in Section 2, the Parties will discuss such additional requirements and the additional fees/charges applicable thereto, and if additional or different rights are agreed, the Parties will enter into a specific written agreement with respect thereto. In this Section, "**Government Agency**" shall mean a national, federal, provincial, state, municipal, and/or local governmental agency or entity in the Territory that acquires Products from Trend Micro under this Agreement for use by such Government Agency.

**19. WEEE Directive.** Trend Micro complies with the WEEE regulations. For information on the disposal of electronic waste, visit <http://uk.trendmicro-europe.com/recycle>.

**20. Force Majeure.** Excusable delays shall be governed by GSA Schedule Contract Clause 552.212-4(f) .

**21. No Third Party Beneficiaries.** To the maximum extent permissible by written waiver, disclaimer, limitation, and/or exclusion under Applicable Laws, this Agreement is entered into solely between and for the benefit of, and may be enforced only by, the Parties hereto and no third party shall have any right/benefit hereunder, whether arising hereunder, under any statute now or hereafter enacted (such as Contracts (Rights of Third Parties) Act of 1999 in the UK and similar laws enacted in Ireland, Singapore, New Zealand, Hong Kong S.A.R., and certain states of Australia, the application of each of which is hereby barred and disclaimed), or otherwise. This Agreement does not, and shall not be deemed to, create any express or implied rights, remedies, benefits, claims, or causes of action (legal, equitable or otherwise) in or on behalf of any third parties including employees, independent consultants, agents, and Affiliates of a Party, or otherwise create any obligation or duty to any third party; *provided, however*, notwithstanding anything contained herein this Agreement to the contrary, Trend Micro's hardware suppliers, software licensors, and Resellers shall be intended third party beneficiaries for the exclusions, limitations, and disclaimers with respect to Products as stated in Sections 7.2, 11.4, and 12 of this Agreement.

**22. Term; Expiration/Termination.** This Agreement and the license rights granted hereunder to: (1) any Standalone Software or Test Software licensed for a Subscription Period shall remain in effect until the term of the license (as may be reflected on the applicable License Certificate) automatically expires; but (2) any Standalone Software (and any Updates thereto purchased by Company) that is licensed for a Perpetual Period shall continue to be licensed indefinitely hereunder (each a "**Term**"); *provided, however*, the Term is subject to earlier termination by either Party as set forth in this Section or elsewhere in this Agreement. Company may terminate this Agreement as to any or all Software licensed hereunder for any or no reason, effective upon notice to Trend Micro..

Upon expiration or earlier termination of this Agreement as to all or a portion (as the case may be) of Software licensed hereunder, the licenses granted hereunder to such expiring or terminating Software (and its Documentation) shall immediately terminate, and Company shall immediately cease use thereof and will uninstall and destroy all copies of the Software (and Documentation) and certify the same to Trend Micro in writing. No expiration or termination shall affect Company's obligation to pay all charges and fees that may have become due before such expiration or termination, or entitle Company to any partial or full refund of amounts already received by Trend Micro, except as specifically set forth in Sections 11.1 and 13.3.

**23. Trend Micro Licensing Entity; Governing Law; Dispute Resolution; Arbitration; Venue/Jurisdiction.**

**231 General; Trend Micro Licensing Entity.** The Parties agree that the specific Trend Micro entity that is the Party to this Agreement for each individual transaction shall be the Trend Micro entity/Affiliated that is stipulated below and such entity shall be conclusively be deemed for all purposes, to be the Trend Micro Party to this Agreement and to the Data Processing Addendum, and the publisher/licensor of Software, supplier of Appliances, and/or provider of Maintenance, that is procured by Company hereunder (in each instance, the "**Licensing Entity**"). The Parties agree that the governing law (without giving effect to its rules and principles relating to conflict of laws) as determine and agreed in this Section 23 shall solely and exclusively apply to and govern, interpret, and sets forth all of Trend Micro's and Company's respective rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this Agreement and the Products provided/secured hereunder. The United Nations Convention on Contracts for the International Sale of Goods does not apply to, and is specifically excluded from application hereto, in any event or circumstance.

**232 North America:** If Company is located (as evidenced by the License Certificate) in the United States of America or Canada, the Licensing Entity of Product is stipulated as: Trend Micro Incorporated, 225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA. The Parties agree that this Agreement is solely and exclusively governed by the Federal laws of the USA. The Parties agree that the provisions of the Uniform Computer Information Transactions Act ("**UCITA**"), as it may have been or hereafter may be in effect in any jurisdiction, shall not apply to this Agreement, and the Parties waive any and all rights they may have under any laws(s) adopting UCITA in any form.

**233 Reserved.**

234      Reserved.

235      Reserved.

236      Reserved.

237      Reserved.

238      Reserved.

239      Reserved.

2310      Reserved.



**TERMS OF SERVICE FOR TREND MICRO CLOUD SERVICES  
THAT ARE HOSTED BY OR ON BEHALF OF TREND MICRO  
(these "Terms of Service")**

**IMPORTANT: READ CAREFULLY. THE RIGHT TO ACCESS AND USE EACH OF TREND MICRO'S CLOUD SERVICES BY BUSINESS, GOVERNMENTAL, AND OTHER LEGAL ENTITIES ARE SUBJECT TO AND CONDITIONED ON ACCEPTANCE OF AND AGREEMENT TO THESE TERMS OF SERVICE. CLOUD SERVICES ARE NOT AVAILABLE FOR PERSONAL USE, HOME USE, AND/OR CONSUMER USE. IF COMPANY AND TREND MICRO HAVE ENTERED INTO A MANUAL/ELECTRONIC SIGNATURE-BEARING CORPORATE LICENSE AGREEMENT (OR OTHER SIMILAR DOCUMENT) WITH RESPECT TO THE ACCESS TO AND/OR USE OF ANY TREND MICRO CLOUD SERVICE, THEN SUCH AGREEMENT WILL GOVERN AND CONTROL THE ACCESS TO AND/OR USE OF SUCH CLOUD SERVICE AND THESE TERMS OF SERVICE WILL HAVE NO EFFECT WITH RESPECT THERETO. OTHERWISE, THESE TERMS OF SERVICE SHALL GOVERN AND CONTROL COMPANY'S ACCESS TO AND/OR USE OF ANY CLOUD SERVICE ACQUIRED HEREUNDER. Any additional, conflicting, or different terms or conditions proposed by Company in any Company-issued document (such as an Order), are hereby rejected by Trend Micro and excluded herefrom.**

**Trial and Paid Use:** Cloud Services are made available by Trend Micro from time-to-time through its Resellers or directly from Trend Micro, but Cloud Services are not available or sold for personal use, home use, and/or consumer use by any person.

**Product Exclusions:** **These Terms of Service do NOT apply to: (a) any standalone application software whether or not acquired from a Reseller, direct from Trend Micro, or an Online Store Provider (as defined in Section 1.2 below) store; (b) any integrated application software that is embedded in or preloaded on a hardware-based appliance; or (c) any annual maintenance for such software licensed by Trend Micro, it being understood that the terms and conditions governing those different Trend Micro products are set forth in the Global Business Software and Appliance Agreement at [trendmicro.com/eula](https://trendmicro.com/eula).**

**Effective Date:** 1 January 2021

**COMPANY IS ORDERING OR HAS ORDERED A CLOUD SERVICE THROUGH COMPANY'S RESELLER OR DIRECTLY FROM TREND MICRO FOR ACCESS AND USE IN CONNECTION WITH COMPANY'S INTERNAL BUSINESS USE. BY COMPANY: (1) ORDERING A CLOUD SERVICE; (2) RESERVED; AND/OR (3) RESERVED:**

- a. COMPANY'S ACKNOWLEDGEMENT THAT IT HAS HAD THE OPPORTUNITY TO READ AND REVIEW THESE TERMS OF SERVICE;
- b. COMPANY'S ACCEPTANCE AND AGREEMENT TO THESE TERMS OF SERVICE FOR SUCH CLOUD SERVICE;
- c. COMPANY'S ONGOING REPRESENTATION AND WARRANTY TO TREND MICRO THAT COMPANY MEETS (AND AT ALL TIMES WILL COMPLY WITH) ALL OF THE TERMS, CONDITIONS, AND REQUIREMENTS SET FORTH IN THESE TERMS OF SERVICE; AND
- d. COMPANY'S REPRESENTATION AND WARRANTY TO TREND MICRO THAT COMPANY'S REPRESENTATIVE ACTING ON ITS BEHALF IS AUTHORIZED TO AND DOES POSSESS THE AUTHORITY TO ACCEPT, AGREE, AND BIND COMPANY TO THESE TERMS OF SERVICE.

**IF COMPANY DOES NOT ACCEPT AND AGREE TO THESE TERMS OF SERVICE, COMPANY MAY NOT ORDER, REGISTER, DEPLOY, ACCESS, OR USE A CLOUD SERVICE AND COMPANY WILL IMMEDIATELY NOTIFY TREND MICRO AT [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com) THAT COMPANY DOES NOT AGREE TO THESE TERMS OF SERVICE AND WILL NOT BE ACCESSING OR USING SUCH CLOUD SERVICE. AGREED DEFINITIONS USED IN THESE TERMS OF SERVICE ARE IN SECTION 1.2 BELOW.**

**1. Overview; Agreed Definitions.**

**1.1.1 Application of These Terms of Service.** Subject always to termination in accordance herewith, these Terms of Service that have been accepted and agreed by Company are applicable only to the Cloud Service for such time that the Cloud Service is subject to an outstanding Order that Company has issued directly or indirectly to, and has been accepted by, Trend Micro.

**1.1.2 Entire Agreement.** The Company and Trend Micro agree that these Terms of Service (including the Standard Contractual Clauses and Data Processing Addendum that form a part hereof and set forth certain of the responsibilities of the Parties with respect to GDPR Data) are the final, complete, and exclusive statement of the agreement between the Parties with respect to access to and use of the Cloud Service secured by Company under an Order, and any prior agreements, representations, statements, white papers, or advertisement of Trend Micro (whether oral, written, or website) or otherwise arising from any course of dealing between the Parties or usage of the trade or descriptions that are not specifically set forth in these Terms of Service with respect to the subject matter hereof, are all merged into and superseded by these Terms of

Service. Trend Micro will not be bound by, and specifically objects to, any term, condition or other provision that is different from or in addition to the provisions of these Terms of Service (whether or not it would materially alter these Terms of Service) and which is submitted by Company in any Order, confirmation, correspondence or other document. **In entering into these Terms of Service, each Party represents and warrants to the other Party that it is NOT relying on any extrinsic representation, warranty, guarantee, condition, covenant, promise, forbearance, or inducement of any kind or nature that is or was made by any person that is not specifically set forth in these Terms of Service.**

**1.1.3 Procurement Under these Terms of Service.** Company may secure Cloud Services under these Terms of Service by one of two methods:

a. **Procurement Through a Reseller.** Typically, Company will secure a Quote for Cloud Services from a Reseller of Trend Micro products or services. Based on such Quote, Orders by Company will be sent to the Reseller at such prices, discounts, and on invoice and payment terms as agreed solely by Company and its Reseller. Company understands that if an Order is placed with a Reseller, the Reseller can place an order with Trend Micro for Cloud Services (either directly through Trend Micro or through a Trend Micro distributor) as requested by Company. Except for the matters agreed in the first sentence of this paragraph between the Reseller and Company, all other rights, obligations, terms, conditions, limitations, and exclusions regarding Cloud Services that are purchased by Company are exclusively set forth in these Terms of Service. All payments by Company for Cloud Services Ordered from a Reseller will only be made directly to the Reseller and never to Trend Micro. Company acknowledges that each Reseller is an independent contractor and in no event or circumstance will any Reseller now or hereafter be deemed a joint venturer, partner, fiduciary, or agent of Trend Micro. No Reseller has been, or will ever be, authorized or permitted to have a right to create any binding obligation, responsibility, duty, liability, condition, warranty, guaranty, or any otherwise contract for or act on behalf of Trend Micro or waive or renounce any right of Trend Micro or modify any right, obligation, or agreement of Company set forth in these Terms of Service.

b. **Direct Purchase from Trend Micro.** Company may (if permitted by Trend Micro) secure a Quote directly from, and place an Order directly with, Trend Micro based on such Quote, which Order if accepted by Trend Micro will be governed solely by the terms, conditions, limitations, and exclusions set forth in these Terms of Service (including the Certificate). All prices and payment terms will be as set forth in the Quote by Trend Micro in accordance with the GSA Schedule Pricelist and all payments for Cloud Services will be made by Company directly to Trend Micro on such payment terms as set forth in such Quote.

**1.1.4 Not a Master Purchase Agreement.** Company acknowledges that this is NOT a master purchase agreement for subsequent purchases of a Cloud Service, but rather, these Terms of Service only apply to the instant Order of a Cloud Service by Company. Each subsequent Order of Cloud Service placed by Company will be made subject to and conditioned on the agreement of the Parties these Terms of Service unless otherwise agreed in a writing signed by the Parties.

**1.2 Agreed Definitions.** In addition to initially capitalized definitions, descriptions, clarifications, and agreements that may be set forth elsewhere in these Terms of Service (including all policies, procedures, and Trend Micro websites that are specifically referenced and incorporated herein), the initially capitalized definitions, descriptions, clarifications, and agreements shall have the meanings set forth in this Section 1.2 (each is an **"Agreed Definition"**) and all Agreed Definitions shall be equally applicable to the singular, plural, and derivative forms.

**"Administrator"** means one or more Company employees with authorization to manage the Cloud Service on behalf of Company. Each Administrator will have the ability to, among other things, develop Company's Configuration from time-to-time, maintain, set rules and policies for, manage Company's access to, view alerts and events generated by, and/or provide technical support for, all or part of Cloud Service as determined by Company from time-to-time.

**"Affiliate"** means as to a Party, each person that is Controlled by a Party, that Controls such Party, or that is under common Control with such Party. **"Control"** means the direct or indirect ownership of more than fifty percent (50%) of the equity shares or interests (or the maximum equity ownership permitted by Applicable Law if such Party is not permitted to own more than 50%) entitled to vote for the directors or other management of such Party or the equivalent, but only for as long as such ownership relationship continues to exist. Upon request, each Party agrees to confirm in writing to the other Party, the status of any or all Affiliates.

**"Applicable Laws"** means all mandatory national, federal, provincial, state, municipal, and local laws, statutes, acts, ordinances, regulations, rules, codes, treaties, executive orders, supervisory requirements, official directives, circulars, opinions, interpretive letters, and other official releases in the Territory that are applicable from time-to-time to a Party's performance of its obligations and/or exercise of its rights hereunder, including, but not limited to, data protection/privacy laws; corrupt activities/illegal payment laws; economic/trade sanctions rules and regulations; and export/import laws.

**"Certificate"** means a written (electronic or otherwise) acceptance/entitlement confirmation issued by Trend Micro that confirms the Cloud Services purchased by Company hereunder, including the applicable Service Capacity where applicable. The Certificate and these Terms of Service forms the entire agreement between Trend Micro and Company with respect to each Cloud Service that is purchased hereunder. Company is advised to retain the Certificate as proof of its entitlement to such Cloud Service(s). In some regions covered hereby, the Certificate is sometimes referred to as a License Certificate or an Entitlement Certificate.

**"Cloud Service(s)"** means any Trend Micro-branded combination of hardware, software components, and/or any fixed scope, technical/managed service that form the environment of a cloud security service (including any Enabling Software and any infrastructure/platform forming a part thereof that is hosted by or on behalf of Trend Micro in the provision of such Cloud Service) that is accessed and/or used by Company in accordance with Terms of Service for the Service Capacity (as evidenced on the Certificate) that Company has purchased directly from Trend Micro or indirectly from a Reseller. Each Cloud Service also includes any Service Description related to such Cloud Service, Enabling Software (if any), and/or any fixed scope, technical/managed service, as well as any and all content, work product, error corrections; updates; upgrades; new versions; or other releases forming a part of such Cloud Service arising from Support Services or otherwise; and all content and functionality available from Trend Micro support site(s) that Trend Micro may elect to make available to customers of such Cloud Service. For the avoidance of doubt, these Terms of Service do not grant Company any right to request or receive a binary code copy of any Trend Micro published software except for Enabling Software (if any) that may form a part of a Cloud Service.

“**Cloud Service Feedback**” shall have the meaning set forth in [Section 6.2](#).

“**Company**” refers to an entity that: (a) has agreed to these Terms of Service with respect to Cloud Service; (b) has purchased and then-currently has the right to access and/or use (only in accordance with these Terms of Service) Cloud Service hereunder as evidenced by a Certificate; and (c) to which these Terms of Service have not been terminated or otherwise expired.

“**Company’s Configuration**” shall have the meaning set forth in [Section 4.1.3](#).

“**Company Data**” means any and all content, materials, data, and information: (a) uploaded or transmitted by or on behalf of the Company to the Cloud Service environment provided hereunder; and/or (b) otherwise provided or made available to Trend Micro in the course of the Company’s use or access to or receipt of Cloud Services or Support Services.

“**Confidential Information**” shall have the meaning set forth in [Section 6.1](#).

“**Contractor**” is an independent contractor that provides services in support of Company and/or its Affiliates with respect to any Cloud Service provided hereunder pursuant to a written agreement between such Contractor and Company that imposes an obligation (among other obligations) on such Contractor to fully comply with these Terms of Service to the extent of access to and/or use of any Cloud Service by such Contractor.

“**Controlled Technology**” shall have the meaning set forth in [Section 11.4](#).

“**Cyberthreat Data**” means any malware, spyware, virus, worm, Trojan horse, ransomware, or other potentially malicious or harmful code or files that Company does not want, as well as URLs, DNS data, network telemetry, commands, executable binary files, macros, scripts, processes or techniques, metadata, or other information or data associated with the foregoing, that may be related to unauthorized intrusions or attacks by third parties associated therewith and that: (a) Company provides to Trend Micro in connection with these Terms of Service; or (b) is accessed, collected, or discovered by Trend Micro during the course of providing any Cloud Service, excluding any such information or data that identifies Company or to the extent that it includes Personal Data. Cyberthreat Data is not Confidential Information or Company Data hereunder.

“**Data Processing Addendum**” or “**Addendum**” means Trend Micro’s Data Processing Addendum (at [trendmicro.com/dpa](https://trendmicro.com/dpa) and attached hereto) or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)) that is applicable if and to the extent Trend Micro acts as a ‘processor’ or ‘sub-processor’ (as defined in the GDPR) for Company of GDPR Data. The Parties agree that the Data Processing Addendum and the Standard Contractual Clauses that form a part thereof are incorporated herein and made a part hereof for all purposes on the terms and subject to the conditions and limitations set forth herein and therein.

“**Different Terms**” shall have the meaning set forth in [Section 2.2](#).

“**Enabling Software**” means binary code software agent, client, or tool that may be published by Trend Micro from time-to-time and licensed (but never sold) hereunder that is installed on Company’s device(s) that enables and facilitates optimal access to and use of a Cloud Service (such as a management console or user interface), and that does not perform functionality without the active right to access and use Cloud Service. Enabling Software may or may not be identified in the Service Description.

“**End User**” means any individual, entity, or person (directly or indirectly through another user) that: (a) accesses or uses a Cloud Service for Company’s (or an Affiliate’s) benefit in accordance with these Terms of Service such as Company’s Administrator(s), technical/support resources, or employees/contractors whose access/use is in furtherance of Company’s or an Affiliate’s Internal Business Use; or (b) otherwise accesses or uses Cloud Service.

“**Evaluation Service**” shall have the meaning set forth in [Section 2.3](#).

“**Excluded Damages**” means any and all claims, causes of action, losses, expenses, or damages of Company and/or its Affiliates arising from or related to any: loss of use of any networks, systems, software, hardware, computers, or devices; unauthorized access to, alteration of, or the deletion, destruction, corruption, damage, loss, of any information/data and/or the restoration thereof; lost or anticipated business revenue or profits; loss of business opportunity or failure to realize expected savings; third party claim against Company and/or any of its Affiliates; reduction in reputation, or goodwill; loss of use or other downtime of all or a portion of a Cloud Service (or supporting hosting platform) for any reason, including as a result of power outages, system failures, internet failures, or other denial of access to or interruption of such Cloud Service; procurement of substitute goods, software or services; or otherwise for any other incidental, punitive, exemplary, indirect, special, or consequential damages.

“**Excused Performance Events**” means any event, condition, and/or circumstance beyond Trend Micro’s reasonable control that was unavoidable even if foreseeable, including, without limitation: acts of God; declared or undeclared war; terrorism; sabotage; criminal actions; armed conflict; actions of civil authorities or governments; earthquakes; fires; floods; cyber-attacks; network intrusions; “zero day” threats or attacks; private or state-actor hacking, denial-of-service attacks, or other malicious actions; telecom/internet congestion, slowdown or outage; computer, networks, or systems failures or delays involving hardware, software, or services not within Trend Micro’s possession, control and responsibility; or labor strike, embargo, or boycott.

“**GDPR**” means the European Union General Data Protection Regulation that is only applicable to Personal Data that is subject to, regulated by, and protected under the GDPR and shall also include additional laws, rules, and regulations now or hereafter promulgated by the European Union, any Member State, or other governmental authority under or supplemental to the GDPR, as the same may be amended,

supplemented or replaced from time to time; and ‘controller,’ ‘processor,’ and ‘data subject’ shall have the meanings respectively assigned to them in the GDPR.

“**GDPR Data**” shall mean ‘personal data’ (as defined in Art. 4 of the GDPR) under the GDPR that is made available or supplied by Company to Trend Micro pursuant to these Terms of Service, if and only to the extent that the GDPR applies to Trend Micro with respect to its processing of such Personal Data.

“**Global Privacy Notice**” means Trend Micro’s Global Privacy Notice published from time-to-time at [https://www.trendmicro.com/en\\_us/about/legal/privacy-policy-product.html](https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html) and attached hereto or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com).

“**High-Risk Environment**” means a device, situation, environment, network, or system requiring safety design, features, and/or functionality for fail-safe or fault-tolerant operation or execution in order to maintain safe and secure performance in an environment where a failure could lead (directly or indirectly) to bodily injury, death, physical property damage, and/or environmental damage. High-Risk Environments may include, but are not be limited to: (a) the design, construction, operation, or maintenance of any nuclear facility, civil infrastructure such as power plants and waterworks, manufacturing facilities, and/or industrial plants such as chemical refineries; (b) navigation, communications, or operating systems in aircraft, ships, trains, and other modes of transportation; (c) air traffic control systems; (d) weapons systems (nuclear or otherwise); (e) operation of life-support or life-critical medical equipment or other equipment or systems affecting a patient’s health or well-being; or (f) any other device, environment, network, or system in which the unavailability, inaccuracy, circumvention, ineffectiveness, or failure of the Cloud Service could lead or contribute to bodily injury, death, physical property damage, and/or environmental damage.

“**Instance**” means an image of software that is created by executing the software’s setup or install procedure or by duplicating such an image.

“**Internal Business Use**” means the internal business access and use of Cloud Services solely by and for the direct benefit of Company specifically in connection with the security, protection, and/or integrity of Company’s systems, networks, devices, documents, emails, and/or other Company Data.

“**IP Claim**” means any suit, cause of action, or other legal proceeding filed/brought against Company by a third party in the courts of law, equity, or otherwise ONLY in the Territory, that asserts that Company’s use of a Cloud Service (or component parts thereof, but not Open Source Software) provided hereunder directly infringes any patent, copyright, or trademark of such third party, or makes unlawful use of a trade secret of such third party; *provided, however*, the term IP Claim will not include and Trend Micro will have no obligation hereunder unless each and every third party allegation or assertion is specifically made against such Cloud Service alone. In addition, the term IP Claim will not include, and Trend Micro will have no obligation under Section 10 or otherwise with respect to, any suit, claim, cause of action, or other legal proceeding arising out of, based on, or related to the following: (a) any use of Cloud Service by Company that is NOT in accordance with these Terms of Service, its Service Description, or Applicable Laws; (b) Company Data and/or other materials that Company provides or makes available in connection with its use of Cloud Service; (c) any redistribution of Cloud Service, or use of Cloud Service for the benefit of any third party not specifically permitted herein; (d) any use of a version of any Enabling Software that has been superseded and made available to Company, if the IP Claim would have been avoided by using an unaltered current version of such Enabling Software; (e) any Open Source Software; or (f) any third party allegation or assertion made against a Cloud Service (or any output thereof) that involves use of such Cloud Service by Company in combination with any other software, service, business process, or technology not provided by Trend Micro or not specified as being required by the applicable Service Description where the IP Claim would not have arisen or would have been avoided but for such combination.

“**Online Store Provider**” means an entity that hosts an online marketplace or store (each a “**Store**”) that offers for sale: (a) such entity’s infrastructure (IaaS) and/or platform (PaaS) hosting services by separate agreement and a separately-stated service fee with the customer (such as Company); together with (b) the software applications of third party publishers (such as Trend Micro) that are offered and resold (for a separately-stated royalty/fee) by such Online Store Provider for deployment on the Store’s infrastructure and/or platform, but licensed to the customer by the application software publisher for a limited term and not perpetually. Company acknowledges and agrees that license to deploy, access, and use Trend Micro application software that is procured by Company on an Online Store Provider’s store is NOT subject to these Terms of Service.

“**Open Source Software**” means: (a) each and every third party software code/component that is licensed/distributed under a license agreement approved by the Open Source Initiative or similar open source or freeware license (and not these Terms of Service); and (b) is included in a Cloud Service or any Enabling Software by Trend Micro; including any of the following Open Source Initiative-approved license agreements: (i) GNU’s General Public License (GPL), Lesser/Library GPL (LGPL), and GNU Affero Public License; (ii) The Artistic License (i.e., PERL); (iii) the Mozilla Public License; (iv) the Netscape Public License; (v) the Berkeley software design (BSD license including Free BSD or BSD-style license); (vi) the Sun Community Source License (SCSL); (vii) an Open Source Foundation License (e.g., CDE and Motif UNIX user interfaces); (viii) the Apache Server license; or (ix) the MIT License. For the avoidance of doubt, each individual, third party software code/component of Open Source Software has its own copyright and its own license agreement.

“**Optional Features**” means those capabilities, features, and functionality in a Cloud Service that require Trend Micro to process certain Company Data (some of which may be GDPR Data or Personal Data) that Company may elect to opt-in or opt-out of the use thereof only if and to the extent a right to opt-in or opt-out is described in and permitted by its Service Description. For example, such Optional Features if active may permit a Cloud Service to: (a) provide the defined capabilities, features, and functionality thereof as described in the Service Description; and/or (b) provide the most effective, up-to-the-minute threat protection and features to detect or prevent the latest malicious behavior and potentially fraudulent websites, internet security risks, and/or Cyberthreat Data.

“**Order**” means: (a) a purchase order or other ordering document issued by Company in response to a Quote; or (b) a Company-initiated procurement document, in each instance placed by Company (with a Reseller or Trend Micro, as the case may be) for the procurement of Cloud

Services to be supplied only in accordance with and subject to the provisions of these Terms of Service. All Orders are Customer's irrevocable commitment to purchase and pay for the Cloud Services stated in the Order and are subject to direct or indirect acceptance by Trend Micro at its sole discretion, which acceptance occurs and is signified by Trend Micro's issuance of a Certificate to Company for such Cloud Services or other Trend Micro performance signifying its acceptance.

**"Party"** means only each of Company and Trend Micro, and together, they are collectively the only **"Parties."** All other persons are third parties.

**"Personal Data"** means one or more data elements relating to an identified or identifiable natural person that can be used to identify, directly or indirectly, such natural person to the extent such data is regulated, protected, restricted, or controlled under Applicable Laws (such as, for example, the GDPR) for the protection of that natural person's privacy and related rights.

**"Quote(s)"** means one or more documents issued by Trend Micro or its Reseller (as the case may be) to Company specifying the Cloud Service that Company seeks to obtain, the related pricing, payment terms, and offered Service Capacity and sufficient other information to complete the transaction. Each Quote shall incorporate these Terms of Service (specifically, by reference, and/or publication of Trend Micro's website) as the sole basis and governing document for any procurement by Company based on the Quote.

**"Reseller"** means a reseller, Online Store Provider (in limited instances where specifically noted by the Store), system integrator, independent software vendor, VAR, OEM or other channel partner that is authorized by Trend Micro or its distributor to secure orders for the sale of Cloud Services to customers, including Company.

**"Sandboxing"** means a separate, secured code execution environment hosted by Trend Micro that permits it to inspect Cloud Service-selected Company Data for suspected Cyberthreat Data.

**"Service Capacity"** means the applicable Subscription Period together with the number of Virtual Machines, Instances, End Users, throughput volume, email addresses, nodes, other measure, and/or other metering mechanism for each Cloud Service purchased under these Terms of Service that is reflected the Certificate therefor. If a Cloud Service permits Company to exceed the Service Capacity that is purchased by Company, then Company is responsible for promptly purchasing an additional quantity to true-up for any excess usage.

**"Service Description"** means the printed, electronic, and/or online technical documentation and operating instructions and requirements generally made available by Trend Micro for a Cloud Service (and Enabling Software, if any) that is made available to Company for the purpose of supporting Company's Internal Business Use of such Cloud Service. The Service Description is incorporated herein and made a part hereof for all purposes; *provided, however*, Company understands and agrees that the published Service Description may be revised from time-to-time by Trend Micro at its discretion, for among other reasons, changes or improvements to, or new versions of, Cloud Service, without the need to amend these Terms of Service, and in each such event, such revised Service Description will supersede all prior Service Descriptions with respect to subsequent use of such Cloud Service. Trend Micro states that certain Cloud Services may be subject to service level targets, service level objectives, or service level agreements that may be published or otherwise made available by Trend Micro from time-to-time.

**"Smart Protection Network" or "SPN"** means Trend Micro's Smart Protection Network.

**"Standard Contractual Clauses" or "Clauses"** or sometimes also referred to the "EU Model Clauses" means the Standard Contractual Clauses (processors) published by the European Commission, which Standard Contractual Clauses are attached to the Data Processing Addendum attached hereto as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com).

**"Subscription Period"** means the period (such as per host hour, month, or year, but never perpetually) for which Company has purchased the right to access and use a Cloud Service provided hereunder. The Subscription Period is as stated in the Certificate.

**"Support Services"** are described in [Section 5.1](#).

**"Term"** is described in [Section 9.1](#).

**"Territory"** means worldwide other than Japan, subject always to and limited by the terms, conditions, waivers, limitations, disclaimers, and exclusions in these Terms of Service, and present and future Applicable Laws that applies to the Cloud Services and/or the performance of either Party hereunder that prohibits or restricts a Cloud Service sale, use, or access: (a) to certain technology/goods/services; (b) to specified countries; and/or (c) by defined persons.

**"Trend Micro"** means in each instance that Cloud Services are acquired under these Terms of Service, the Licensing Entity that provides Cloud Services in such instance as determined by application of [Section 12](#).

**"Virtual Machine"** means a software container, implementation, or emulation of a computer/server/machine (*i.e.*, a physical device) that runs its own operating system and executes application programs like a physical machine.

## **2. Grant for Cloud Service; License to Enabling Software; Open Source; Security Acknowledgement; Evaluation.**

### **2.1 Grant.**

**2.1.1 Grant of Access to and Use of Cloud Service.** On the terms and subject to Company's continuous compliance with all of the agreements, conditions, exclusions, and restrictions set forth in these Terms of Service (including the Certificate), Trend Micro hereby grants only to Company, a non-exclusive, non-transferable, non-assignable, terminable (in accordance herewith or Applicable Law) limited right in the Territory to access and use Cloud Service in accordance with its Service Description only for Company's Internal Business Use (and the Internal

Business Use of any of its Affiliates and/or Contractors as it permits in accordance with Section 2.11) for such time and only for the Service Capacity purchased and paid for (in accordance with agreed payment terms) by Company until the expiration or termination of the foregoing grant in accordance herewith. Company may allow access to and use a Cloud Service only for the purposes specifically permitted herein including the Service Description.

**2.1.2 License to Enabling Software.** If a Cloud Service is accompanied by Enabling Software, then by downloading or installing any Enabling Software on any computer, Company agrees not to use such Enabling Software for any purpose other than to facilitate and/or enable Company's access to and use of such Cloud Service. Subject to these Terms of Service, Trend Micro grants Company (solely for the Internal Business Use of Company except as otherwise permitted in Section 2.11) a non-exclusive, non-transferable, worldwide (subject to Applicable Laws), terminable (in accordance herewith) license to install and use any Enabling Software on equipment owned or operated by or on behalf of Company, solely as needed to access and/or use Cloud Service as described in the Service Description; *provided that*, Company: (a) at all times complies with the terms and conditions of these Terms of Service and the Service Description; (b) ensures that anyone (including End Users) who accesses or uses the Enabling Software (accessed either locally or remotely) in connection with Cloud Service (i) does so only on Company's (or an Affiliate's if permitted by Company) behalf and for its sole benefit, and (ii) complies with the terms and conditions of these Terms of Service; (c) does not (i) install, access, use, copy, modify, or distribute the Enabling Software except as may be expressly permitted in Service Description and these Terms of Service, and/or (ii) reverse assemble, reverse compile, otherwise translate, or reverse engineer the Enabling Software; and (d) does not use any of the Enabling Software's components, files, modules, or related licensed materials separately from the Enabling Software. Company acknowledges that the Enabling Software is copyrighted and licensed and not sold to Company under the terms of these Terms of Service and Company acknowledges that it is not hereunder granted any license, right, title, or interest in or to any patent, copyright, trade secret or other intellectual property of Trend Micro or any third party. All rights in and to Enabling Software not expressly granted to Company in this Section 2.1.2 are reserved by Trend Micro and Company will have no other or different rights (implied, by estoppel, or otherwise) or privileges with respect to any Enabling Software. If and to the extent only as maybe permitted in the Service Description, Company may make a single copy of the Enabling Software for back-up, archival, and disaster recovery purposes. The Enabling Software (and every back-up, archive, and disaster recovery copy) must be promptly un-installed and irretrievably destroyed when Company no longer has a right to access or use a Cloud Service provided hereunder.

**2.2 Open Source Software.** Enabling Software may come bundled or otherwise be distributed with Open Source Software, that is subject solely to the agreement terms, conditions, limitations, and disclaimers of the specific license (each "**Different Terms**") under which such Open Source Software is distributed by Trend Micro in such Enabling Code and NOT these Terms of Service. Different Terms, if any, applicable to any Open Source Software redistributed in any Enabling Software provided hereunder will be identified by Trend Micro in the Service Description for, and/or in a "Read Me" or an "About" file in, the Enabling Software. OPEN SOURCE SOFTWARE IS PROVIDED BY TREND MICRO "AS IS, WITH ALL FAULTS, AS AVAILABLE" WITHOUT (AND TREND MICRO SPECIFICALLY DISCLAIMS) ANY GUARANTEE, CONDITION, OR WARRANTY (EXPRESS, IMPLIED, OR OTHERWISE) OF ANY KIND OR NATURE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, TITLE, AND/OR NON-INFRINGEMENT. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THESE TERMS OF SERVICE, AS IT RELATES TO ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH OPEN SOURCE SOFTWARE, TREND MICRO SHALL HAVE NO LIABILITY FOR ANY DIRECT OR EXCLUDED DAMAGES, HOWSOEVER CAUSED AND/OR OTHERWISE BASED ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF OPEN SOURCE SOFTWARE, EVEN IF TREND MICRO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**2.3 Evaluation of Cloud Service.** If Company has Ordered and agreed to these Terms of Service or otherwise entitled to an evaluation, trial, proof-of-concept, or test of a Cloud Service (herein "**Evaluation Service**"), then the provisions of this Section shall apply and shall control over any conflicting terms of these Terms of Service. On the terms and subject to the conditions of these Terms of Service when and if accepted and approved by Trend Micro, Company will have the right to conduct a test of the Evaluation Service for a period not to exceed thirty (30) days (unless otherwise agreed to in writing by Trend Micro or earlier terminated in accordance with Sections 9 or 10), during which period Company may access and use the Evaluation Service solely for Company's internal evaluation in a non-production environment (that is to say, an environment that does not access or process any live production Company Data or otherwise perform productive work) to decide whether to purchase the right to continue to access and use the Evaluation Service for its Internal Business Use. Evaluation Services are provided gratuitously by Trend Micro. Trend Micro has no obligation to provide any training or Support Service for the Evaluation Service, but Trend Micro may do so at its sole discretion. Company acknowledges that the Evaluation Service may contain errors, defects or other problems that could cause system or other failures, security breaches, interruptions, and/or data loss. CONSEQUENTLY, EVALUATION SERVICES ARE PROVIDED TO COMPANY SOLELY ON "**AS AVAILABLE**" AND "**AS IS, WITH ALL FAULTS**" BASIS, AND TREND MICRO DISCLAIMS ALL WARRANTIES, CONDITIONS, GUARANTEES, AND LIABILITY IN CONNECTION WITH ALL EVALUATION SERVICES. COMPANY ASSUMES ALL RISK OF USE OF EVALUATION SERVICES. WHERE LEGAL LIABILITY CANNOT BE EXCLUDED, BUT MAY BE LIMITED, THE LIABILITY OF TREND MICRO, ITS LICENSORS, AND/OR SUPPLIERS SHALL BE LIMITED TO THE SUM OF ONE HUNDRED UNITED STATES DOLLARS (USD\$100.00) IN THE AGGREGATE FOR ALL CLAIMS AND CAUSES OF ACTION. If Company accesses and/or uses Cloud Service after expiration of Evaluation Services as set forth in this Section 2.3, Company agrees to pay for Cloud Service thereafter in accordance with the GSA Schedule Pricelist and the Parties agree that these Terms of Service shall apply to such paid use.

**2.4 Security Acknowledgement.** Certain portions of Cloud Services are designed to identify, block and/or remove applications, messages, and files that may compromise productivity or the performance and security of computers, systems, and/or networks. While Trend Micro uses commercially reasonable efforts to properly identify applications and files for detection by its Cloud Services, *however*, given the constantly changing nature and volume of malicious, fraudulent, and unwanted electronic content, Trend Micro cannot and does not represent, warrant, or guarantee that a Cloud Service will detect, block, or completely remove or clean any or all applications, routines, and files that are malicious, fraudulent, or that Company does not use or want. Company understands and agrees that the success of its security efforts are dependent on a number of factors solely under Company's control and responsibility such as: (a) use of a number of network, hardware, cloud services, and software security tools in a coordinated effort to manage present and future security threats; (b) implementation of cybersecurity protocols and controls, network, cloud services and systems protections, as well as monitoring and detection processes applicable to the foregoing; (c) enforcement

of appropriate internal security policies, procedures, and controls regarding access, security, encryption, use, and transmission of data; (d) the development and continual testing of processes and procedures (i) for the backup and recovery of any network, system, software, database, and any stored data, as well as, (ii) implementation of security-breach incident response practices; (e) conducting regular cybersecurity and privacy training for employees; (f) having adequate vendor risk management processes; and (g) promptly downloading and installing all updates to all networks, products, and software that are made available to Company by any publisher or manufacturer.

**2.5 Ownership; Reservation of Rights.** Each Cloud Service is and remains the exclusive property of Trend Micro and/or its licensors and service providers. Except for Company's limited access and use rights expressly granted in these Terms of Service and the limited license granted in [Section 2.1.2](#) to Enabling Software, no license, right, title, or interest in or to a Cloud Service or Trend Micro's and its licensor's intellectual property rights therein, are granted to Company. Company acknowledges and agrees that, as between the Parties, each Cloud Service and all ideas, methods, algorithms, formulae, processes, and concepts incorporated into Cloud Service, and all revisions, corrections, modifications, enhancements, derivative works, releases, and upgrades, and anything developed (such as performance of an analysis of and any all Cyberthreat Data provided with Company Data to a Cloud Service) or made available by or on behalf of Trend Micro under these Terms of Service and/or a Cloud Service, and any copies of the foregoing are: (a) the intellectual property of Trend Micro, its Affiliates, and/or its or their licensors/suppliers; and (b) all right, title, and interest therein are reserved to and the sole property of Trend Micro, its licensors, and/or such other persons as Trend Micro may determine. Company will not alter or remove Trend Micro's and its licensors' copyright notices and all other proprietary legends from any part of Cloud Service.

**2.6 Changes and Improvements to Cloud Service.** Trend Micro reserves the right (at its discretion and without notice to or consent of any person) to continually improve, update, and offer new versions of Cloud Service (e.g., infrastructure/platform, features or functionality, security, technical configurations, and/or application features) during the Term, to reflect changes in, among other things, laws, regulations, rules, technology, industry practices, patterns of use, and cyberthreat environment and capabilities. Any such improvement, change, and/or new version of Cloud Service shall be governed by these Terms of Service and shall not be treated as a breach. Company acknowledges that the use of some of which may be contingent upon Company's agreement to additional terms. In the event that Trend Micro discontinues or materially diminishes functionality of a Service that Company has contracted for, Company shall be entitled to a pro rata refund for any fees paid not used.

**2.7 End-of-Life.** Trend Micro reserves the right to discontinue the publication, sale, distribution, subscription, licensing, and support of any or all Cloud Services at any time and for any reason (each event herein "End-of-Life") by announcement or publication of notice to the general public or revision of its price list. Please refer to Trend Micro's then-current End-of-Life Policies and a then-current list of Cloud Services subject to an End-of-Life notice at <https://success.trendmicro.com/support-policies>. The Parties agree that an End-of-Life announcement of any Cloud Service shall not be considered a breach hereof by Trend Micro, nor shall any such End-of-Life entitle Company to any claim for compensation or damages as result of or in connection therewith.

**2.8 Acceptable Use.** Company will not make any use or disclosure of, or perform any acts with respect to, Cloud Service other than as expressly permitted by its Service Description or these Terms of Service. Company may not and agrees that it will not as its material obligation hereunder (and any non-compliance with or breach thereof is a material breach by Company of these Terms of Service), nor will Company authorize, encourage, or permit third parties to:

- (a) Disable, tamper with, or otherwise attempt to circumvent any billing mechanism that meters Company's use of a Cloud Service or otherwise use a Cloud Service in a way intended to avoid incurring fees or exceeding the Service Capacity limitations in Certificate or otherwise attempt to gain unauthorized access to a Cloud Service.
- (b) Access or use any Cloud Service without permission in accordance herewith, including attempting to probe, scan, or test the vulnerability of the environment of any Cloud Service or to breach any security or authentication measures used by or in such Cloud Service.
- (c) Modify, adapt, copy (except as may be expressly permitted herein with respect to Enabling Software), translate, disassemble, decompile, or reverse engineer Cloud Service (or any of its components or parts thereof), or otherwise attempt to derive the source code of, decrypt, modify, or create derivative works of, Cloud Service or any part thereof; *provided, however*, configuring a Cloud Service within its policy parameters set forth in the Service Description to create Company's Configuration shall not constitute a modification or derivative work.
- (d) License, sublicense, sell, resell, loan, rent, lease, transfer, assign, distribute, or provide the benefit of any Cloud Service (or any portion thereof) to any third party except as specifically set forth in [Section 2.11](#).
- (e) Use Cloud Service: (i) as a paid or unpaid service bureau or otherwise to provide services directly or indirectly to third parties (such as business processing outsourcing); (ii) to provide services to third parties on a time-share basis; or (iii) otherwise commercially exploit or make Cloud Service available to any third party save as set forth in [Section 2.11](#).
- (f) Access, evaluate, observe, or use a Cloud Service (or any of its components) to build or support (or assist a third party in building or supporting) the improvement and/or creation of a competitive product or service, or copy any ideas, features, functions, organization, structure, graphics, or user interface of Cloud Service for any reason.
- (g) Use a Cloud Service: (i) in a manner that violates Applicable Laws or otherwise to engage in or promote any illegal, harmful, fraudulent, offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, or offensive; (ii) in a manner that infringes or misappropriates the intellectual property rights of any third party or otherwise that breaches these Terms of Service; (iii) interfere with the use of Cloud Services by any third party; or (iv) interfere with the proper functioning of the equipment and environment used to provide Cloud Services.
- (h) Publish or otherwise make available to any third party, any benchmark tests or performance analysis relating to Cloud Service without the express written permission of Trend Micro which may be withheld or conditioned at the sole discretion of Trend Micro.

In addition to any other rights or remedies afforded to Trend Micro under these Term of Service or under any Applicable Law, Trend Micro reserves the right, but has no obligation, to investigate suspected violations of undertakings in this Section or any misuse of a Cloud Service and to take remedial action if Company breaches or violates any of the foregoing commitments, including the suspension, removal, or disablement of access to such Cloud Service by Company in accordance with the Disputes Clause (Contract Disputes Act). In addition, Company agrees that Trend Micro may report any activity that it suspects violates any Applicable

Law to the appropriate law or regulatory enforcement officials and provide any assistance required under such Applicable Law. Trend Micro shall have no liability to Company for damages or anything else in the event that Trend Micro takes any such action in good faith.

**2.9 High-Risk Environment.** Cloud Services are not fault-tolerant/fail-safe and are not intended, designed, tested, or certified to be reliable or suitable for use in High-Risk Environments and Trend Micro specifically disclaims any express or implied warranty/condition/guarantee of fitness for use of any Cloud Service in a High-Risk Environment. Trend Micro notifies Company that no Cloud Service has been submitted for compliance testing, certification, or approval for any use by any governmental agency and/or a self-regulatory, standard-setting, or other industry/product-specific consensus organization in a High-Risk Environment. As a condition to Company utilizing any Cloud Service in a High-Risk Environment, Company agrees to: (1) secure and maintain any and all certifications and/or approvals required under any Applicable Law with respect to a Cloud Service that Company intends to deploy in a High-Risk Environment; and (2) undertake all appropriate and/or necessary testing, fail-safe, backup, redundancy and other measures necessary to ensure the safe deployment and use of any Cloud Service by Company in a High-Risk Environment. Any access, deployment, or use of any Cloud Service in a High-Risk Environment shall be at Company's sole liability and risk and Company does hereby irrevocably waive and renounce any and all claims or causes of action for losses, expenses, or damages (of every kind and nature) that Company and its Affiliates may now or hereafter have against Trend Micro and its Affiliates with respect to Company's access, deployment, or use of any Cloud Service in a High-Risk Environment.

**2.10 Applicable Laws.** To the extent applicable to Company's performance of its obligations and/or exercise of its rights hereunder (including without limitation in relation to Company's and its Affiliates' (and its and their Contractors') use and/or configuration of any Cloud Service), Company represents (on an ongoing basis) and warrants to Trend Micro and agrees that Company and its Affiliates' (and its and their Contractors') will: (a) comply with all Applicable Laws (including, without limitation, the GDPR if and to the extent applicable) and will not use or configure any Cloud Service or give any instructions to Trend Micro which would or could infringe, violate, or otherwise not be in compliance with any Applicable Laws or could cause Trend Micro to do so; and (b) identify, procure, and maintain any permits, certificates, approvals, consents, and inspections that may be required or advisable in order to comply with Applicable Laws with respect hereto. If there is any failure to comply with or breach of these Terms of Service arising out of or related to this Section, Company will promptly (at no cost Trend Micro) do all things and take all actions as may be necessary or appropriate to cure and correct any breach or non-compliance with any Applicable Laws.

**2.11 Affiliate and/or Contractor Use.** For no more than the Service Capacity purchased by or on behalf of Company as evidenced in a Certificate, Trend Micro grants Company the right to authorize and permit (for no additional fees or amounts due Trend Micro other than the fees already payable with respect to the rights granted to Company): (a) Company's Affiliates to access and/or utilize Cloud Services only in connection with such Affiliate's Internal Business Use for so long as such person remains an Affiliate of Company; and (b) Contractors to Company and/or its Affiliates to access and/or utilize Cloud Services only in connection with the provision of business process support, technical support, hosting services, and/or outsourcing services to and solely for the use and benefit of Company and/or Affiliates in connection with its and their Internal Business Use and not for the benefit of any third party or such Contractor, all of the foregoing on the terms and subject to the limitations and conditions of these Terms of Service. Each Affiliate and Contractor having access to, possession of, and/or utilization of any Cloud Service will be considered an authorized user of Company under these Terms of Service with respect to such Cloud Service and NOT having any rights or deemed to be a third party beneficiary hereunder in any event or circumstance. Company agrees at all times to require, ensure, and enforce compliance with the grants, terms, conditions, and limitations set forth in these Terms of Service as well as the Data Processing Addendum and Standard Contractual Clauses where applicable by Company's Affiliates (including, without limitation, those applicable to the Affiliate's GDPR Data that may be exported outside of the EEA to Trend Micro by the Affiliate's use of any Cloud Service purchased by Company) and/or Contractors having access to Cloud Services procured hereunder and, further, Company agrees that it shall at all times be and remain legally and financially responsible to Trend Micro for the compliance and non-compliance with, or breach of, these Terms of Service (and the Standard the Data Processing Addendum/Contractual Clauses where applicable) directly or indirectly caused by any Affiliate or Contractor. For the avoidance of doubt, since all Support Services are to be provided by Trend Micro only to Company, no Affiliate and/or Contractor will be entitled to request or receive Support Services directly from Trend Micro.

### **3. Company Responsibilities.**

**3.1 Cloud Service Setup; Registration; Administrators.** Company is responsible for architecting, selecting, configuring, registering, and securing operation of, as well as securing and maintaining connectivity and access to, Cloud Service. Company must provide Trend Micro with all necessary or advisable information to allow Trend Micro to provision and make available Cloud Service, as well as permit registration that requires, among other things, an entity name and address, primary contact name and information, an email address, and other information as may be requested by Trend Micro from time-to-time. Registration information will be treated as the Confidential Information of Company. In accordance with the Service Description, Company will provide to Trend Micro (and maintain), contact information for Company's Administrator(s) who are the only End Users authorized or permitted to provide information required to manage, create Company's Configuration, as well as request and undertake Support Services of a Cloud Service for Company.

**3.2 Authentication Credentials.** Company has sole control over access and use by its End Users, Affiliates, and Contractors of a Cloud Service, and is responsible for ALL activity (whether authorized or unauthorized) occurring on Company's Cloud Service account hereunder. Company is responsible for maintaining the confidentiality of any non-public authentication credentials associated with its access to and use of a Cloud Service. Company will ensure that all End Users comply with Company's obligations under these Terms of Service and that the terms and conditions of Company's agreement with each End User are consistent with these Terms of Service. If Company becomes aware of any breach or non-compliance of Company's obligations under these Terms of Service by an End User or other third party such as an Affiliate or Contractor, Company will immediately terminate such person's access to Cloud Service and notify Trend Micro. Further, Company is solely responsible for population, maintenance, security, protection, loss prevention, and backup of Company's systems and networks, Company Data, and other content, information, and devices.

**3.3 Internet Transmission.** Company understands and agrees that no data transmission over the Internet by Company is guaranteed to be secure by Trend Micro. Trend Micro is not responsible for any interception or interruption of any communications through the Internet or networks or systems outside Trend Micro's control. Company is solely responsible for maintaining the security of its networks, servers, applications and access codes.

**3.4 Fees.** Company will timely pay to its Reseller or directly to Trend Micro, as the case may be, the applicable fees for access to and/or use of Cloud Service in accordance with the Service Capacity that is purchased by Company. Invoicing and collection of the fees and any applicable Taxes will be by its Reseller or directly by Trend Micro, as the case may be.

**3.5 Taxes – Direct Orders.** Trend Micro or its authorized reseller as applicable shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). If Company is legally entitled to an exemption from the collection and remittance of any otherwise applicable Taxes, Company is responsible for providing Trend Micro with legally-sufficient tax exemption certificates for each taxing jurisdiction. Otherwise, Company will be invoiced for, and pay, all Taxes as required to be collected by Trend Micro under Applicable Law.

**3.6 Compliance; Audit.** Trend Micro may request, and Company will provide within thirty (30) days from the request date, a system-generated report verifying Company's access to and use of the Cloud Services, if and only if, a Cloud Service purchased hereunder is programmed with the technological features to provide such access and use verification (including Service Capacity where applicable). In any event, Trend Micro has the right, at its expense, to audit Company's compliance with these Terms of Service, and Company will provide all records and information reasonably necessary for Trend Micro to successfully perform such audit. If any audit reveals that Company owes fees to Trend Micro, or its Reseller, Company will promptly remit such underpaid amounts within thirty (30) days of receipt of a proper invoice. Company consents to Trend Micro's disclosure of such audit results to the Reseller.

#### **4. Company Data; Optional Features; Personal Data Protection; GDPR Data Processing.**

##### **4.1 Responsibility for Company Data; Right to Use Company Data; Optional Features.**

**4.1.1 Responsibility for Company Data.** Company is solely responsible for the content of all Company Data and represents to Trend Micro (on an ongoing basis) and agrees to the extent required by Applicable Law or any agreement of Company with a third party, that Company will: (a) with respect to all Company Data, provide all notices to, and procure and maintain all necessary rights, consents, and approvals; and (b) take any and all other actions as may be required, to ensure the lawfulness of Company's access to and/or use of each Cloud Service (and applicable Support Services), including without limitation its transmission or making available of Company Data (some of which may include Personal Data) to Trend Micro and Trend Micro's receipt and use of such Company Data in that connection, without Company in any such case violating any Applicable Laws or the rights of any third party or otherwise obligating Trend Micro to any third party. Trend Micro does not and will not assume any obligations to Company with respect to Company Data or Company's use of Cloud Service other than as may be expressly set forth in these Terms of Service including in relation to its provision of Support Services.

**4.1.2 Right to Use Company Data.** Company hereby grants Trend Micro a limited, non-exclusive, royalty-free, paid-up, license to access and use Company Data (unless and only to the extent Company opts-out of such uses through Company's Configuration): (a) as necessary for Trend Micro to provide each Cloud Service and provide Support Services to Company; (b) to maintain and improve the operation, security efficacy, and functionality of Trend Micro's software and services including Cloud Services; (c) to identify and collect information on potential security risks and URLs associated with websites, executable files, or content identified as potential malware vectors in order to continually provide Cloud Services and to improve Trend Micro's subject-matter databases; (d) for administration of these Terms of Service and each Cloud Service; (e) to comply with its legal obligations and exercise its rights under Applicable Laws; and (f) for other purposes set forth in these Terms of Service and/or Trend Micro's Global Privacy Notice.

**4.1.3 Company's Configuration.** Company acknowledges and agrees that a Cloud Service may contain certain Optional Features. Company is solely responsible for selecting (during activation/initial deployment and at all times thereafter) and maintaining Company's Configuration of each Cloud Service and assuring that Company's Configuration conforms to Company's requirements, policies, and procedures regarding any processing of Company Data (including any GDPR Data and/or other Personal Data) and complies with all Applicable Laws in each jurisdiction to which Company's processing of any Company Data in connection with its use of any Cloud Service may be subject (including any GDPR Data and/or Personal Data) and/or from which Company is accessing and utilizing an Optional Feature. At the initial activation and deployment of each Cloud Service and at any time thereafter, Company agrees to: (a) review the capabilities, features, and functionality of the Optional Features and all other features and functionality in the Service Description thereof; and (b) activate, configure, restrict, limit, and/or disable each Optional Feature as may be described in the Service Description in order to cause Company Data to be processed in a manner that meets Company's specific needs (each Cloud Service as configured by or on behalf of Company from time-to-time is herein referred to as "**Company's Configuration**"). Except for Optional Features and permissions and administrative selections described in the Service Description, Company understands that each Cloud Service is a standardized service hosted by or on behalf of Trend Micro and no additional or different instructions or configurations are available to Company for such Cloud Service.

**4.2 Personal Data Protection.** A Cloud Service and/or Support Services may employ applications and tools that receive Company Data that includes one or more data elements that are Personal Data under Applicable Laws. In accordance with the instructions made known through Company's Configuration and these Terms of Service, Trend Micro may access, receive, process, copy, backup, store, transfer and use Personal Data which may take place in, from and to the United States of America, Europe, or other countries or jurisdictions, potentially outside of the country of residence of Company, its Affiliates, and/or its and their End Users. Trend Micro has and will continue to implement technical, organizational and administrative security measures in order to protect the Personal Data provided to and utilized in connection with each Cloud Service from unauthorized access and misuse while under Trend Micro's custody or control, including when Trend Micro utilizes any third party

subcontractors. Trend Micro restricts its personnel from accessing and/or utilizing Personal Data without authorization and imposes appropriate obligations upon its personnel regarding Personal Data protection.

**4.3 GDPR Data Processing; Relationship of the Parties.** By agreeing to these Terms of Service, each of Company and Trend Micro acknowledges and agrees that it is also entering into and agreeing to be bound by: (a) the Data Processing Addendum; and (b) the Standard Contractual Clauses, it being further agreed that each of the Addendum and Clauses shall only apply, if and to the extent that Trend Micro acts as a processor or subprocessor for any GDPR Data (but does not apply to other Company Data/Personal Data) that Company (and its Affiliates that have been authorized to access and/or utilize Cloud Services hereunder) provides or makes available to Trend Micro hereunder. Customer shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States. With respect to each Affiliate of Company that accesses or utilizes any Cloud Service as permitted herein, Company hereby enters into and agrees to be bound by the Data Processing Addendum and the Standard Contractual Clauses for itself and on behalf of each such Affiliate, and Company represents and warrants to Trend Micro that Company is duly authorized, and Company and all such Affiliates have each taken, all necessary action to do so validly.

## **5. Support Services; Updates to Enabling Software.**

**5.1 Support Services.** Trend Micro will provide Support Services for each Cloud Service to Company in connection herewith on the terms, conditions, and descriptions set forth in the Support Services terms provided to Company, subject to the conditions stated in such Support Service Description (the “**Support Services**”). Service Level Targets for Support Services may be found at [www.trendmicro.com/severitydefinitions](http://www.trendmicro.com/severitydefinitions), which Service Level Targets may be revised by Trend Micro at its discretion from time-to-time. Except for the Support Services, these Terms of Service do not require Trend Micro to provide Company with any configuration, deployment, training, consulting services, or other technical assistance of any kind. Each Cloud Service is periodically monitored by Trend Micro based on its Service Level Targets and adjustments are made by Trend Micro as needed.

**5.2 Updates to Enabling Software.** At its sole discretion, Trend Micro may provide periodic updates to the Enabling Software, if any. If available, such updates may include bug fixes, new features and/or enhancements. Company is solely responsible for deploying such updates at Company’s own cost as soon as possible. Trend Micro’s obligation to provide Support Services with respect to Enabling Software as well as a Cloud Service continuing to meet its Service Description and these Terms of Service depends upon Company’s prompt installation of any and all such updates to Enabling Software that Trend Micro makes available to Company.

## **6. Confidentiality; Feedback.**

**6.1 Confidentiality/Non-Disclosure.** Each Party hereto acknowledges that by reason of its relationship with the other Party hereunder, it may have access to confidential information and materials concerning the other Party’s business, technology, and/or products that is confidential to the other Party (“**Confidential Information**”). Written or other tangible Confidential Information must at the time of disclosure be identified and labeled as Confidential Information belonging to the disclosing Party. When disclosed orally or visually, Confidential Information must be identified as confidential at the time of the disclosure, with subsequent confirmation in writing within fifteen (15) days after disclosure. Each Party agrees that it will not use such Confidential Information, except as authorized under these Terms of Service, and will protect Confidential Information at least to the same extent as a reasonable person would undertake to protect such Confidential Information. Neither Party may use the other Party’s Confidential Information except to perform its duties or exercise its rights under these Terms of Service. The Confidential Information restrictions will not apply to information or data that is: (a) already known to the receiving Party at the time of access hereunder; (b) becomes publicly available through no wrongful act of the receiving Party; (c) independently developed by the receiving Party without benefit of the disclosing Party’s Confidential Information; (d) has been rightfully received from a third party not under obligation of confidentiality; (e) disclosed in any legal proceeding arising from or in connection with these Terms of Service; or (f) is required to be disclosed by law, provided the Party compelled to disclose the Confidential Information provides the Party owning the Confidential Information with prior written notice of disclosure (only if legally permissible) adequate for the owning Party to take reasonable action to prevent such disclosure. Unless otherwise agreed to by both Parties, upon termination of these Terms of Service, each Party will return to, or irretrievably destroy, the other Party’s Confidential Information in its possession. **In the event that the Parties hereto have previously entered into a non-disclosure or confidentiality agreement that is still in effect on the Effective Date of these Terms of Service, then the Parties hereto agree that such prior agreement is hereby merged into and superseded by these Terms of Service ONLY with respect to the subject matter hereof and the transactions undertaken pursuant hereto.** Trend Micro recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as “confidential” by the vendor.

## **6.2**

## **7. Limited Warranty and Exclusive Remedy; Disclaimer of All Other Conditions, Guarantees, and Warranties.**

**7.1 Limited Warranty and Exclusive Remedy.** In connection with a Cloud Service, Trend Micro warrants only to Company that such Cloud Service will substantially conform to its then-current Service Description under normal use and circumstances until the expiration or termination of Company’s paid right to access and use such Cloud Service under these Terms of Service. The foregoing limited warranty does not cover events or circumstances caused by accident, abuse or use of Cloud Service in a manner inconsistent with these Terms of Service, the Service Description, or other guidance provided by Trend Micro or resulting from events of Force Majeure. If it is established that Trend Micro has breached the above warranty after notice from Company as required below, Trend Micro may, at its option: (a) use reasonable efforts to cure the breach; or (b) in the event Trend Micro cannot, after commercially practicable attempts to do so, achieve the remedy in (a) immediately above, either Trend Micro or Company may terminate these Terms of Service and Trend Micro will provide a refund (within thirty (30) days) of unused

fees pre-paid by Company, if any, as of the effective date of such termination. To benefit from this warranty and the remedies stated herein, Company must report in writing to Trend Micro, the alleged breach of warranty with reasonable specificity within ten (10) days of its occurrence. The above remedies for breach of the foregoing warranty are Trend Micro's sole and exclusive obligation and liability to Company and Company's sole and exclusive right and remedy for Trend Micro's breach of the foregoing warranty notwithstanding any other provision of these Terms of Service to the contrary.

**7.2 Disclaimer of All Other Conditions, Guarantees, and Warranties.** EXCEPT AS SET FORTH IN SECTION 7.1, CLOUD SERVICES AND SUPPORT SERVICES ARE PROVIDED "AS IS, WITH ALL FAULTS" AND "AS AVAILABLE" AND WITHOUT ANY OTHER WARRANTY, CONDITION, UNDERTAKING, OR GUARANTEE OF ANY KIND OR NATURE. TREND MICRO (ON BEHALF OF ITSELF AND ITS AFFILIATES/SUPPLIERS/LICENSORS/RESELLERS) EXPRESSLY DISCLAIMS ALL REPRESENTATIONS, GUARANTEES, CONDITIONS, UNDERTAKINGS, OR WARRANTIES OF ANY KIND (WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) ARISING FROM OR RELATED TO A STATUTE, CIVIL/COMMERCIAL CODE, CUSTOM, USAGE OR TRADE PRACTICE, COURSE OF DEALING OR PERFORMANCE, OR THE PARTIES' CONDUCT OR COMMUNICATIONS WITH ONE ANOTHER, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AND/OR CONDITION OF: MERCHANTABILITY; FITNESS FOR A PARTICULAR (SUCH AS A HIGH-RISK ENVIRONMENT) OR GENERAL PURPOSE; TITLE; SATISFACTORY QUALITY; ACCURACY; NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS; OR ABILITY TO ACHIEVE A PARTICULAR RESULT. FURTHER, TREND MICRO DOES NOT REPRESENT, WARRANT, OR GUARANTEE THAT: (A) A CLOUD SERVICE WILL BE CONTINUOUSLY AVAILABLE OR USE THEREOF UNINTERRUPTED; (B) THE FUNCTIONS AND FEATURES CONTAINED IN A CLOUD SERVICE WILL MEET THE REQUIREMENTS OF COMPANY OR THAT A CLOUD SERVICE WILL SATISFY ANY PARTICULAR BUSINESS, TECHNOLOGICAL, SERVICE, SECURITY, OR OTHER NEEDS OR REQUIREMENTS (SUCH AS USE IN A HIGH-RISK ENVIRONMENT) OF COMPANY; (C) USE OF A CLOUD SERVICE WILL PROVIDE COMPLETE AND ABSOLUTE PROTECTION OF COMPANY'S SYSTEMS, NETWORKS, DEVICES, ASSETS, INFORMATION, AND/OR DATA FROM AND AGAINST ANY OR ALL CYBERTHREAT DATA OR OTHER POSSIBLE RISKS; (D) USE OF A CLOUD SERVICE WILL DETECT, IDENTIFY, BLOCK, REMOVE, REMEDIATE, OR RESOLVE SOME, ANY, OR ALL CYBERTHREAT DATA; (E) A CLOUD SERVICE WILL BE PROVIDED OR PERFORMED ERROR-FREE OR THAT TREND MICRO WILL CORRECT ALL ERRORS IN CLOUD SERVICES; OR (F) A CLOUD SERVICE WILL OPERATE IN COMBINATION WITH COMPANY DATA, OR WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEMS, CLOUD SERVICES, OR DATA NOT PROVIDED OR REQUIRED BY TREND MICRO.

## **8. Exclusions From and Limitation of Liability; Maximum Liability.**

**8.1 Exclusions From and Limitation of Liability.** IN NO EVENT OR CIRCUMSTANCE WILL TREND MICRO (OR ITS AFFILIATES, LICENSORS, OR SUPPLIERS) BE LIABLE TO COMPANY OR ITS AFFILIATES FOR ANY EXCLUDED DAMAGES ARISING FROM OR RELATING TO THESE TERMS OF SERVICE, TREND MICRO'S (OR ITS AFFILIATES) PERFORMANCE UNDER THESE TERMS OF SERVICE, OR ANY CLOUD SERVICE/SUPPORT SERVICE, WHETHER OR NOT FORESEEABLE, EVEN IF THE EXCLUSIVE REMEDIES PROVIDED BY THESE TERMS OF SERVICE FAIL OF THEIR ESSENTIAL PURPOSE AND EVEN IF TREND MICRO AND/OR ITS AFFILIATES MAY HAVE BEEN ADVISED OF THE POSSIBILITY OR PROBABILITY OF SUCH DAMAGES AND REGARDLESS OF THE NATURE OF THE CLAIM OR CAUSE OF ACTION OR THEORY ASSERTED INCLUDING, WITHOUT LIMITATION; BREACH OF CONTRACT; STRICT LIABILITY; MISREPRESENTATION; UNDER ANY EXPRESS/IMPLIED/STATUTORY WARRANTY, GUARANTEE, DUTY, OR CONDITION; UNDER ANY STATUTE OR CIVIL/COMMERCIAL CODE; IN TORT (INCLUDING NEGLIGENCE); OR ANY OTHER LEGAL, IMPLIED, STATUTORY, OR EQUITABLE THEORY. THE PARTIES AGREE THAT NONE OF THE EXCLUDED DAMAGES REFERENCED IN THIS SECTION 8.1 ARE ACTUAL DIRECT DAMAGES AS REFERENCED IN SECTION 8.2. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

IF COMPANY IS IN THE EUROPEAN ECONOMIC AREA, REFERENCES TO "EXCLUDED DAMAGES" SHALL ALSO MEAN ANY LOSSES OR DAMAGES WHICH: (A) WERE NOT REASONABLY FORESEEABLE BY BOTH PARTIES; (B) WERE KNOWN TO COMPANY BUT NOT TO TREND MICRO; AND/OR (C) WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED BY COMPANY SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO COMPANY DATA OR COMPANY'S FAILURE TO PROPERLY BACK-UP SUCH COMPANY DATA.

**8.2 Maximum Liability – Actual Direct Damages.** THE LIABILITY OF TREND MICRO, ITS AFFILIATES, AND ITS THEIR SUPPLIERS (INCLUDING ANY HOSTING PLATFORM) AND LICENSORS TO COMPANY FOR LOSSES, EXPENSES, OR DAMAGES RELATED TO OR ARISING FROM ALL RELATED AND UNRELATED CAUSES OF ACTION, CLAIMS, SUITS, AND OTHER LEGAL PROCEEDINGS OF ANY KIND OR NATURE (REGARDLESS OF WHETHER BASED ON EXPRESS/IMPLIED/STATUTORY WARRANTY, GUARANTEE, CONDITION, MISREPRESENTATION, CONTRACT AND BREACH THEREOF, STRICT LIABILITY, TORT (INCLUDING NEGLIGENCE), UNDER ANY CIVIL/COMMERCIAL CODE, AND/OR ANY OTHER OR EQUITABLE OR LEGAL THEORY) THAT ARE ACTS OR OMISSIONS OF TREND MICRO SPECIFICALLY ATTRIBUTABLE TO: (A) AN UNCURED MATERIAL BREACH OF THESE TERMS OF SERVICE; (B) THE RELATIONSHIP OF PARTIES; AND/OR (C) THE PROVISION/SUPPLY OF CLOUD SERVICES AND/OR SUPPORT SERVICES, SHALL BE LIMITED TO ACTUAL DIRECT DAMAGES IN AN AMOUNT NOT TO EXCEED, IN THE AGGREGATE (AND NOT PER INCIDENT OR PER CLAIMANT) FOR ALL CLAIMS AND CAUSES OF ACTION, THE TOTAL FEES AND OTHER AMOUNTS PAID BY COMPANY FOR THE CLOUD SERVICE GIVING RISE TO OR CAUSING SUCH LOSS, EXPENSE, OR DAMAGE IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO SUCH LOSS, EXPENSE, OR DAMAGE, LESS ANY REFUNDS OR CREDITS PREVIOUSLY RECEIVED BY COMPANY FROM TREND MICRO WITH RESPECT THERETO.

**8.3 Basis of the Bargain.** Each Party recognizes and agrees that the waivers, warranty limitations, as well as disclaimers and exclusions from and limitations of liability and/or remedies in these Terms of Service are a material and essential basis of these Terms

of Service; reflect a reasonable allocation of risk between the Parties; are fair, reasonable, and a fundamental part of these Terms of Service; and each has been taken into account and reflected in determining the consideration to be given by each Party under these Terms of Service and in the decision by each Party to enter into these Terms of Service. The Parties acknowledge and agree that absent any of such waivers, disclaimers, exclusions, and/or limitations of liability/remedies, the provisions of these Terms of Service, including the economic terms, would be substantially different, or in the alternative, these Terms of Service would not have been consummated.

## **9. Term and Termination.**

**9.1 Term.** These Terms of Service and Company's access to Cloud Service will become effective as of the date of issuance of a Certificate to Company by Trend Micro and such Cloud Service is made available to the Company by Trend Micro and shall continue in effect thereafter as set forth in the applicable Certificate and these Terms of Service until such outstanding Subscription Period for a Cloud Service purchased hereunder is completed (the "Term"), unless earlier terminated or suspended in accordance with this Section and/or these Terms of Service.

**9.2 Suspension and Termination by Trend Micro.** Trend Micro may temporarily suspend Company's right to use Cloud Service (in whole or in part) at any time upon written notice if Trend Micro determines that: (a) Company or one or more of its Affiliates, Contractors, or End Users of Cloud Service (i) poses a security risk to Cloud Service or any third party, (ii) may adversely impact Cloud Service or any third party, (iii) reserved, or (iv) reserved. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Trend Micro shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Company will cease use of Cloud Service identified in such notice(s) during any period of suspension, or upon termination of these Terms of Service or other termination of Company's right to use such Cloud Service. For any termination or suspension by Trend Micro in accordance with the foregoing, Trend Micro will not provide, or be liable for, any refund or proration of fees.

**9.3 Termination by Company.** Company may terminate for its convenience, these Terms of Service and/or Company's use of a Cloud Service at any time with written notice to Trend Micro. Notwithstanding the foregoing, only if Company is entitled to terminate these Terms of Service for a material breach by Trend Micro (after giving Trend Micro at least twenty (20) days prior detailed written notice and an opportunity to cure such material breach during such notice period) of these Terms of Service, Company will be entitled to receive a refund from Trend Micro of the applicable unused fees (if any) pre-paid by Company for access to Cloud Service.

**9.4 Company's Termination Duties.** Upon expiration or termination of these Terms of Service and/or Company's use of Cloud Service for any reason or no reason, Company will: (a) cease any access and use of Cloud Service; and (b) irretrievably destroy all copies in Company's possession or control of the Enabling Software, including any Service Description provided by Trend Micro. Upon request, Company will certify in writing that the foregoing has occurred. Termination does not relieve Company from Company's obligation to pay fees and Taxes that remain unpaid.

**9.5 Survival.** Upon termination or expiration of these Terms of Service and regardless of reason therefor, the following Sections shall survive such termination or expiration: Sections 1, 2.2, 2.3, 2.4, 2.5, 2.8, 2.9, 2.10, 2.11, 3, 4, 6, 7, 8, 9, 10, 11, and 12 and any other provision that expressly states that its terms and conditions shall survive the expiration or termination of these Terms of Service.

## **10. Intellectual Property Indemnity.**

**10.1 IP Claim Indemnity.** Trend Micro (at its cost) will have the right to intervene to defend ONLY Company from each IP Claim and indemnify Company from the resulting costs and damages with respect to each such IP Claim finally awarded against Company ONLY that are specifically attributable to such IP Claim or those amounts agreed to by Trend Micro in a monetary settlement of such IP Claim, subject always to the conditions, qualifications and limitations in this Section 10. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. No settlement of any IP Claim will be made by Company (and Trend Micro will have no responsibility or obligation hereunder or otherwise therefor) without Trend Micro's express written consent, which may be withheld at its sole and absolute discretion. The obligation of Trend Micro under this Section 10 for any IP Claim is subject to and conditioned on Company giving Trend Micro: (a) prompt written notice of any IP Claim (but in any event notice in sufficient time for Trend Micro to respond without prejudice to its position), provided that a failure to provide notice shall only relieve Trend Micro of its indemnity obligation to the extent Trend Micro was prejudiced by such failure; (b) sole and complete control and authority over the defense, negotiations, and settlement of such IP Claim; and (c) reasonable requested information, cooperation and assistance, at Trend Micro's expense, with regard to the defense, negotiations, or settlement of such IP Claim. Without Company's consent, Trend Micro will not settle with respect to Company, any IP Claim to the extent such settlement requires that Company admit any liability on the part of Company with respect to such IP Claim or pay any money therefor. Company may participate in the defense of any IP Claim at its cost with counsel of its selection. **This indemnity is personal to Company and may not be assigned/transferred (in whole or in part) or otherwise passed through to any third party.**

**10.2 IP Claim Mitigation.** Should a Cloud Service at any time become, or in Trend Micro's opinion be likely to become, the subject of an IP Claim, Trend Micro shall have the right, at its sole option to: (a) procure for Company the right to continue using such Cloud Service as provided hereunder, or (b) modify such Cloud Service so that it no longer is the subject of an IP Claim, while maintaining substantially the same utility or functionality of the unmodified utility or functionality. If neither (a) or (b) are commercially practicable in Trend Micro's opinion, Trend Micro may terminate these Terms of Service as to such Cloud Service and any related rights granted hereunder to access and utilize the Cloud Service upon written notice, in which event Company will cease further use of the Cloud Service and return or uninstall and irrevocably destroy all copies of any Enabling Software (and its documentation) and, thereafter, Trend Micro will promptly refund to Company any unused, prepaid fees Company may have paid for such Cloud Service. The Parties agree that any termination hereof in accordance with this Section 10 shall not be treated as a breach of these Terms of Service by Trend Micro and shall not entitle Company to any claim for damages, losses, or expenses of any kind or nature arising from or related to such termination including for replacement cost or loss of use of the Cloud Service or any lost profits, savings, or revenue arising from or related to the Cloud Service. **This Section 10 states Trend Micro's sole and exclusive obligation and liability to Company, and Company's sole and exclusive right and remedy against Trend Micro, for any IP Claim. Except as set forth herein this Section 10, Company acknowledges and agrees that no indemnity is given by Trend Micro with respect to any Cloud Service and Trend**

Micro specifically denies and disclaims any obligation to indemnify company and/or its affiliates from and against any other matter or thing in any event or circumstance. Notwithstanding anything contained herein to the contrary, Trend Micro's liability shall not be limited by Section 8 to the extent of monies payable by Trend Micro by operation of this Section 10.

## **11. General Provisions.**

**11.1 Assignment, Delegation; Sublicensing; Subcontracting** Company will not assign (in whole or in part) these Terms of Service, or delegate or sublicense any of Company's rights under these Terms of Service, without Trend Micro's prior written consent. Any purported assignment or transfer in violation of this Section 11.1 will be void.. Subject to the foregoing, these Terms of Service will be binding upon, and inure to the benefit of the parties and their respective successors and assigns.

**11.2 Interpretation.** The headings within these Terms of Service are for convenience only and will not affect the interpretation of these Terms of Service. The words "include", "includes", and "including" shall be interpreted as introducing a list of examples which do not limit the generality of any preceding words or any words in the list of examples.

**11.3 No Waivers.** The failure by either Party to enforce any provision of these Terms of Service will not constitute a present or future waiver of such provision nor limit our right to enforce such provision at a later time. To be effective, all waivers must be in writing, specifying the provision and actions or inactions being waived, and signed by the Parties.

**11.4 Export/Import Control.** In connection with these Terms of Service, the access, use, export or re-export of Cloud Service and related technical data and services (collectively "**Controlled Technology**") is subject to Applicable Laws with respect to the export (including "deemed export" and "deemed re-export" regulations) and import of Controlled Technology by Company, its Affiliates, Contractors, and/or its End Users. In connection therewith, Company acknowledges that each Cloud Service is designed with capabilities to permit (at its and their discretion) Company, its Affiliates, Contractors, and/or its End Users to access the Cloud Service without regard to geographic location and to transfer or otherwise move Company Data between the Cloud Service, its Affiliates, Contractors, and/or its End Users/Contractors anywhere in the world. Company acknowledges and agrees that it is solely responsible for the authorization and management of End User accounts, as well as export/import control and geographic transfer of Company Data in connection with the Cloud Service. Company agrees that it will at all times comply with each Applicable Law (now or hereafter in effect) that applies to direct/indirect export, re-export, or import of Controlled Technology by Company, its Affiliates, and its and their Contractors, and/or its End Users and/or the performance of Company, its Affiliates, its or their Contractors, and/or its End Users hereunder that: (a) requires a license to, or otherwise prohibits the, export, re-export, import, diversion, or disclosure of such Controlled Technology; (b) prohibits or restricts sale, use, or access to certain technology/goods/services, to specified countries, and/or by defined persons; or (c) restricts or prohibits end-use of such Controlled Technology related to the development, production, use, or proliferation of nuclear, chemical or biological weapons, missiles, or other weapons of mass destruction. Company represents and warrants to Trend Micro that neither Company, its Affiliates, its Contractors, nor any of its End Users are under the control of, located in, or a resident or national of any country or region subject to any embargo or applicable trade sanction and are not a prohibited person or prohibited entity as defined in any Applicable Law.

**11.5 Government Agency Use.** Each Cloud Service (including any component software) and accompanying Service Description have been developed solely at private expense by Trend Micro and/or its suppliers/licensors, consisting of commercially-available items, commercially-available computer software, commercially-available hardware, technical documentation, and/or commercially-available Service Description with the same rights and restrictions generally applicable to Cloud Service. Access and use of Cloud Service by any Government Agency may be subject to mandatory applicable laws; *provided, however*, except for the limited right to access and use Cloud Service granted in Sections 2.1 above, no right, title, or interest in or to any software, hardware, binary code, or service (or updates and documentation) is granted or transferred hereunder to any Government Agency accessing and/or using Cloud Service. If any Government Agency requires or needs greater or different rights in or to access and/or use Cloud Service other than those rights that are granted in these Terms of Service, the Parties will discuss such additional requirements and the additional fees/charges applicable thereto, and if additional or different rights are agreed, the parties will enter into a specific written agreement with respect thereto. In this Section 11.5, "**Government Agency**" shall mean a national, federal, provincial, state, municipal, and/or local agency or entity that Orders through a Reseller for the right to access/use a Cloud Service under these Terms of Service.

## **11.6 Notices.**

**11.6.1 If to Company.** Trend Micro may provide any notice to Company under these Terms of Service: (a) if a legal notice, by sending a message to the email address then associated with Company's Account, if any; and (b) if product or support notices, by posting a notice on <https://success.trendmicro.com/TechnicalSupport> (the "**Trend Micro Site**"). Product or support notices posted on the Trend Micro Site will be effective upon posting and legal notices that Trend Micro provides by email will be effective when Trend Micro sends the email. It is Company's responsibility to keep Company's email address current.

**11.6.2 If to Trend Micro.** To give Trend Micro legal notice under these Terms of Service, Company must contact Trend Micro by email to [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com). Trend Micro may update the email for notices by posting a notice on the Trend Micro Site. Notices provided by email will be effective one (1) business day after they are sent. Notices regarding Support Services will be sent in accordance with Section 5.1 and notices or Orders regarding new or additional Cloud Services should be directed to the appropriate Reseller or Trend Micro's sales executive, as the case may be.

**11.7 Severability; Enforcement.** The Parties agree that the unenforceability or invalidity of any term or provision of these Terms of Service shall not impair the enforceability or validity of any other part of these Terms of Service. In the event that any term or provision of these Terms of Service conflicts with the governing law under which these Terms of Service is to be construed or if any such term or provision is held invalid or unenforceable in whole or in part by a court with jurisdiction over the Parties or in any arbitration convened hereunder, the Parties agree that the court or arbitrator(s) (as the case may be) making such determination shall have the power, and the Parties hereby request that such court or arbitrator(s) exercise such power, to modify, amend, or restate any such unenforceable term or provision of these Terms of Service in lieu of

severing such unenforceable term or provision in its entirety, whether by rewriting the offending term or provision, deleting any or all of the offending term or provision, adding additional language to these Terms of Service, or by making such other modifications as it deems appropriate that is valid and enforceable and that comes closest to expressing the original intention of the Parties to the greatest lawful extent under these Terms of Service.

**11.8 Excused Performance Events.** In accordance with GSA 552.212-4(f), Trend Micro shall not be liable for any delay or failure to perform its obligations hereunder due to any Excused Performance Event. Trend Micro will (a) take commercially reasonable steps to minimize and/or mitigate any delays or failures related to any Excused Performance Event, and (b) provide prompt written notice of the nature of such Excused Performance Event and the expected duration thereof to Company, but this Section does not excuse Trend Micro's obligation to take reasonable steps to follow its normal disaster recovery procedures. Trend Micro will resume performing its affected obligations promptly following the removal or reasonable circumvention of such Excused Performance Event. The Parties agree that any delay or failure arising from or related to a Excused Performance Event shall not constitute a breach of these Terms of Service by Trend Micro.

**11.9 Independent Contractors.** Nothing in these Terms of Service is intended or shall be construed to create or establish any agency, partnership, or joint venture relationship between the Parties. The Parties expressly disclaim such relationship, agree that they are acting solely as independent contractors hereunder, and agree that the Parties have no fiduciary duty to one another or any other special or implied duties that are not expressly stated herein. Neither Party has any authority to act as agent for, or to incur any obligations on behalf of or in the name of, the other Party or its Affiliates.

**11.10 Third Party Beneficiaries.** Except as set forth in the immediately preceding sentence, these Terms of Service are entered into solely between and for the benefit of, and may be enforced only by, the Parties hereto and no third party shall have any right/benefit hereunder, whether arising hereunder, under any statute now or hereafter enacted (such as Contracts (Rights of Third Parties) Act of 1999 in the UK and similar laws enacted in Ireland, Singapore, New Zealand, Hong Kong S.A.R., and certain states of Australia, the application of each of which is hereby barred and disclaimed), or otherwise. Except as set forth in the first sentence of this Section, these Terms of Service do not, and shall not be deemed to, create any express or implied rights, remedies, benefits, claims, or causes of action (legal, equitable or otherwise) in or on behalf of any third parties including employees, independent consultants, agents, suppliers, and Affiliates of a Party, or otherwise create any obligation or duty to any third party; *provided, however*, notwithstanding anything contained herein these Terms of Service to the contrary, Trend Micro's Affiliates, licensors, and Resellers shall be intended third party beneficiaries for the exclusions, limitations, and disclaimers with respect to Cloud Services as stated in Sections 2.8, 2.9, 7.2, and 8 of these Terms of Service.

## **12. Trend Micro Licensing Entity; Governing Law; Dispute Resolution; Arbitration; Venue/Jurisdiction.**

**12.1 General; Trend Micro Licensing Entity.** The Parties agree that the specific Trend Micro entity that is the Party to these Terms of Service for each individual transaction shall be the Trend Micro entity/Affiliate that is stipulated below and such entity shall be conclusively be deemed for all purposes, to be the Trend Micro Party to these Terms of Service and to the Data Processing Addendum, and the publisher/licensor of Software, supplier of Appliances, and/or provider of Support Services, that is procured by Company hereunder (in each instance, the "**Licensing Entity**"). The Parties agree that the governing law (without giving effect to its rules and principles relating to conflict of laws) as determine and agreed in this Section 12 shall solely and exclusively apply to and govern, interpret, and sets forth all of Trend Micro's and Company's respective rights, duties, and obligations arising from, or relating in any manner to, the subject matter of these Terms of Service and the Cloud Services provided/secured hereunder. The United Nations Convention on Contracts for the International Sale of Goods does not apply to, and is specifically excluded from application hereto, in any event or circumstance.

**12.2 North America:** If Company is located (as evidenced by the Certificate) in the United States of America or Canada, the Licensing Entity of Cloud Service is stipulated as: Trend Micro Incorporated, 225 E. John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA. The Parties agree that these Terms of Service is solely and exclusively governed by the Federal laws of the USA. The Parties agree that the provisions of the Uniform Computer Information Transactions Act ("**UCITA**"), as it may have been or hereafter may be in effect in any jurisdiction, shall not apply to these Terms of Service, and the Parties waive any and all rights they may have under any laws(s) adopting UCITA in any form.

**12.3 Reserved.**

**12.4 Reserved.**

**12.5 Reserved.**

**12.6 Reserved:**

**12.7 Reserved**

**12.8 Reserved.**

**12.9 Reserved.**

**12.10 Reserved.**

**EXHIBIT A**  
**DATA PROCESSING ADDENDUM**  
**(THIS "ADDENDUM")**

**1. Definitions**

1.1 *Definitions; Construction.* Terms defined in any agreement between Company and Trend Micro that incorporates this Addendum by reference (herein each an "**Agreement**") shall have the same meanings when used herein unless superseded or modified by a definition or text herein, in which event the term defined or conflicting text set forth herein shall govern and control. All defined terms shall be equally applicable to the singular, plural, and derivative forms. Certain of the defined terms set forth in this Addendum generally follow the definition in the GDPR and apply to all Personal Data covered herein; *provided, however*, when being read in the context of a specific Personal Data Protection Law, then such definition will be deemed to be the definition (if any) set forth in such specific Personal Data Protection Law and not the definition set forth in this Addendum. References herein to "**Company**" shall include its Affiliates that it permits to access and use any Products or Services under Company's Agreement. For the avoidance of doubt, "**Company**" herein shall not include any Contractor of Company and Trend Micro has no obligations or liabilities hereunder to any Contractors.

"**Company's Configuration**" shall have the meaning set forth in the Agreement.

"**Data Protection Impact Assessment**" shall have the meaning if set forth in, and required by, an applicable Personal Data Protection Law.

"**Data Subject**" means an identified or identifiable natural person whose Personal Data is Processed by Trend Micro in connection herewith and an Agreement.

"**European Data Protection Law**" means: (i) Regulation 2016/679 (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU e-Privacy Directive (Directive 2002/58/EC); (iii) the EU GDPR as it is saved and incorporated into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to apply in the UK under section 2 of the European Union (Withdrawal) Act 2018; and (iv) any and all applicable national data protection law made under, pursuant, supplemental to or in order to give effect to (i) – (iv); in each case as may be amended or superseded from time to time. The following terms shall have the meanings given to them in European Data Protection Law: "Controller", "Data Protection Impact Assessment", "Data Subject", "Process", "Processed", "Processing", "Processor" when referencing Personal Data subject thereto.

"**GDPR**" means the EU GDPR and/or the UK GDPR, as applicable.

"**Global Privacy Notice**" means Trend Micro's Global Privacy Notice published from time-to-time at [https://www.trendmicro.com/en\\_us/about/trust-center/privacy.html](https://www.trendmicro.com/en_us/about/trust-center/privacy.html) or as may be requested by Company from [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com).

"**Party**" means each party to: (1) an Agreement that incorporates this Addendum; and/or (2) this Addendum. All other persons are third parties.

"**Permitted Purposes**" shall have the meaning set forth in clause 2.2.

**"Personal Data"** means one or more data elements relating to an identified or identifiable natural person that can be used to identify, directly or indirectly, such natural person that is made available or supplied by Company to Trend Micro pursuant to the Agreement and this Addendum forming a part thereof and any Personal Data generated or derived in relation to such Personal Data such as logs, if and only to the extent such data elements are regulated, protected, restricted, or controlled under an applicable Personal Data Protection Law(s).

**"Personal Data Protection Law"** means any country/regional (including, national, state/provincial, and local) enacted law that is applicable to a Party's provision, access to, and/or Processing of Personal Data under an Agreement that this Addendum is incorporated into and forms a part of, as may be enacted, amended, or superseded from time-to-time.

**"Processing"** means any operation or set of operations that are performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**"Products"** means software, cloud services (including SaaS products), fixed-scope managed services, and/or hardware-based appliances as may be provided by Trend Micro to Company under the applicable Agreement that incorporates this Addendum.

**"Regulator"** means the independent public authority with responsibility for enforcing Personal Data Protection Laws in a relevant jurisdiction.

**"Security Incident"** shall have the meaning set forth in [clause 3.3](#).

**"Services"** means support, maintenance, and/or unique technical services engagements other than Products to be provided by Trend Micro to Company under the Agreement that incorporates this Addendum.

**"Sub-Processor"** means an entity engaged by Trend Micro to perform certain services as described in [clause 3.4](#).

**"Trend Micro"** means the Trend Micro group company that is the counterparty to the Agreement and this Addendum with Company,

1.2 Application of this Addendum. This Addendum is applicable to any Trend Micro Agreement with Company that specifically incorporates this Addendum as a part thereof and applies to the extent Trend Micro Processes any Personal Data as Processor or Sub-Processor for Company within the scope of an applicable Personal Data Protection Law in connection with providing any Products or Services to Company. The terms and conditions of this Addendum supersede anything to the contrary set forth in the Agreement and governs and controls the rights of the Parties with respect to the subject matter hereof.

1.3 Scope. This Addendum is applicable to all Personal Data that is Processed by Trend Micro under an Agreement. In addition, this Addendum contains certain provisions that are only applicable to Personal Data that is subject to European Data Protection Laws.

## **2. Details of Processing**

2.1 For clarity, this Addendum applies with respect to any Personal Data of which Company is the Controller or Processor within the scope of a Personal Data Protection Law and Trend Micro is Processor or Sub-Processor for Company, as the case may be, of such Personal Data.

2.2 Company appoints and instructs Trend Micro as its Processor or Sub-Processor to Process the Personal Data for the purpose of providing Products or Services to Company as described in the

Agreement (or as otherwise agreed in writing between the Parties) (together the "**Permitted Purposes**").

2.3 Each Party shall comply with its obligations under Personal Data Protection Law in relation to its Processing of such Personal Data.

2.4 The subject matter, duration, nature and purpose of this Processing are as set out in Annex 1 of this Addendum.

### **3. Trend Micro's Obligations Applicable to All Personal Data**

3.1 If and to the extent Trend Micro acts as Processor or Sub-Processor of any Personal Data for the Company, Trend Micro shall only Process the Personal Data for the Permitted Purposes, and only in accordance with Company's documented instructions, unless it is required otherwise by applicable Personal Data Protection Law. Trend Micro will notify Company promptly if it considers (but without being obliged to investigate the legal position), that: (i) it is required by any applicable Personal Data Protection Law to act other than in accordance with any Company instruction, provided that Trend Micro is not prohibited by applicable law from such notification; or (ii) any of Company's instructions infringe or violate Personal Data Protection Law(s). Company agrees and confirms that the Agreement, this Addendum, and Company's Configuration (as defined in the Agreement) together constitute Company's complete and sole instructions to Trend Micro regarding the Personal Data.

3.2 Trend Micro shall ensure that any person it authorizes to process any Personal Data are subject to a duty of confidentiality (whether a contractual or statutory duty) regarding such Personal Data.

3.3 Trend Micro shall implement appropriate and reasonable technical and organizational measures to protect the Personal Data from (i) accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure or access (a "**Security Incident**") to provide a level of security appropriate to the risk using standards of at least those set out in Annex 2 of this Addendum.

3.4 Company consents to Trend Micro engaging third party Sub-Processors to Process the Personal Data for the Permitted Purposes provided that: (i) Trend Micro maintains an up-to-date list of its Sub-Processors at [trendmicro.com/subprocessors](https://trendmicro.com/subprocessors) which it shall update with details of any change in Sub-Processors at least thirty (30) days' prior to any such change; (ii) Trend Micro enters into a written agreement containing data protection obligations with any Sub-Processor it appoints that require the Sub-Processor to protect any Personal Data to at least the standard required by this Addendum; and (iii) Trend Micro remains liable for any failure by its Sub-Processor to fulfil such Personal Data protection obligations (including any breach of this Addendum that is caused by an act, error or omission of its Sub-Processor). Within fourteen (14) days of publication to the above website, Company may object to Trend Micro's appointment or replacement of a Sub-Processor, provided such objection includes Company's reasons therefor that are based solely on reasonable grounds relating to Personal Data protection.

3.5 In the event of the Company's timely objection in accordance with clause 3.4 above:

- (a) Trend Micro may elect to not appoint or to replace such Sub-Processor; or
- (b) if Trend Micro elects to use such Sub-Processor after Company's reasonable objection, Company may terminate the Agreement without penalty with effect from the date that such Sub-Processor change takes effect as to any affected Product or Service as stipulated by Company (it being understood and agreed that such right of termination is Company's sole and exclusive right and remedy if Company objects to any new or replacement Sub-Processor

appointed by Trend Micro and without prejudice to accrued fees or other rights under the Agreement).

3.6 To the extent legally permitted, in connection with Trend Micro's processing of the Personal Data, Trend Micro shall provide reasonable and timely assistance to Company (at Company's expense and subject to Company's payment of Trend Micro's fees for such assistance at its standard professional services rates prevailing at the time) to enable Company to respond to:

- (a) any request from a Data Subject to exercise any of its rights under Personal Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and
- (b) any other correspondence, enquiry or complaint received from a Data Subject, Regulator or other third party.

In the event that any such request, correspondence, enquiry or complaint is made directly to Trend Micro, Trend Micro shall promptly inform Company providing full details of the same to the extent legally permitted. Unless otherwise required by applicable law, Trend Micro shall not disclose any Personal Data in response to any such request without Company's prior written direction.

3.7 Trend Micro shall provide reasonable cooperation to Company (at Company's expense and subject to Company's payment of Trend Micro's fees for such cooperation at its standard professional services rates prevailing at the time) in connection with any Data Protection Impact Assessment that may be required under Personal Data Protection Laws regarding Company's use of the Products and/or Services.

3.8 If it becomes aware of a confirmed Security Incident in relation to any Personal Data, Trend Micro shall inform Company without undue delay and shall provide reasonable information and cooperation to Company so that Company can fulfil any Personal Data breach reporting obligations it may have under (and in accordance with the timescales required by) a Personal Data Protection Law. To the extent Trend Micro or its Sub-Processor caused such Security Incident, Trend Micro shall further take (or require its Sub-Processor to take) any reasonably necessary measures and actions to remedy or mitigate the effects of the Security Incident. Trend Micro shall keep Company informed of all material developments in connection with such Security Incident without undue delay.

3.9 Upon termination or expiry of the Agreement, Trend Micro shall (at Company's election) destroy or return to Company all Personal Data that is in Trend Micro's possession or control (including any copies thereof). This requirement shall not apply to the extent that Trend Micro is required by applicable laws to retain some or all Personal Data, or to Personal Data it has archived on back-up systems, in which event Trend Micro shall securely isolate and protect such Personal Data from any further Processing (except to the extent required by such law) until deletion is possible.

3.10 Trend Micro is committed to making available to Company all information necessary to demonstrate compliance with the obligations laid down in this Addendum and allow for and contribute to audits, including inspections, conducted by Company or another auditor mandated by Company. In this regard, the Parties agree the following:

- (a) Company acknowledges that the operation of Trend Micro's data centers are regularly audited against ISO 27001 standards by independent third-party auditors, and includes 24x7 monitoring services and incident response, infrastructure management, change management, project management, automation tool development and technical consulting services for public cloud deployment in both on-premise data center and any applicable third party hosting

service such as Amazon Web Services. Upon request, Trend Micro shall supply a summary copy of its audit report(s) to Company, which shall be subject to the confidentiality provisions of the Agreement.

- (b) After Company has exercised its rights under paragraph (a) above, if Company requires further information Company will have the right to, at its own cost and subject to Company's payment of Trend Micro's fees in relation to such audit at its standard professional services rates prevailing at the time, require that Trend Micro (or its independent third-party auditors) carry out a bespoke audit in relation to Trend Micro's compliance with this Addendum. Upon receipt of such request, Trend Micro will carry out (or arrange) such audit within such reasonable period as Company and Trend Micro may agree, and will provide a copy of the audit report to Company promptly following conclusion of the audit.

#### **4. Company's obligations.**

##### **4.1 Company shall, in relation to the Personal Data:**

- (a) where required to do so, make notification(s) to any relevant Regulator in relation to its Processing of the Personal Data (including regarding any Security Incident notified to it by Trend Micro) in an objective manner and in such a manner as not to intentionally or unreasonably bring Trend Micro into disrepute or otherwise tarnish the reputation of Trend Micro;
- (b) ensure it is not subject to any prohibition or restriction which would: (i) prevent or restrict it from disclosing or transferring any Personal Data to Trend Micro; (ii) prevent or restrict it from granting Trend Micro access to any Personal Data; and/or (iii) prevent or restrict Trend Micro from Processing any Personal Data, in each case as provided in clause 3 above;
- (c) ensure that all fair Processing notices have been given (and/or, as applicable, consents obtained) in accordance with Personal Data Protection Law and are sufficient in scope to enable Trend Micro to Process the Personal Data as provided in clause 3 above; and
- (d) maintain technical and organizational security measures sufficient to comply at least with the obligations imposed on a Controller by Personal Data Protection Law.
- (e) If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

4.2 Company's instructions for the Processing of Personal Data shall comply with Personal Data Protection Law. Company shall not give any instructions to Trend Micro that may cause Trend Micro to infringe any applicable law.

4.3 Any information or notices to be provided by Trend Micro may be given to Company without having to be given to any of Company's Affiliates also.

#### **5. Provisions Applicable to Specific Personal Data Protection Laws**

##### **5.1 Applicable Only to European Economic Area and the UK Personal Data**

5.1.1 The following terms shall have the following meanings in this clause 5.1.

- (a) **"Restricted Transfer"** means: (i) a transfer of Personal Data that is protected by the EU GDPR to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; or (ii) a transfer of Personal Data that is protected by the UK GDPR to a country outside of the United Kingdom which is not subject to an adequacy determination pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and
- (b) **"Standard Contractual Clauses"** means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**").

5.1.2 Trend Micro shall not transfer any Personal Data outside of the European Economic Area or the United Kingdom unless it has taken such measures as are necessary to ensure the transfer is in compliance with European Data Protection Law. Such measures may include (without limitation) transferring Personal Data to a recipient: (i) in a country that the European Commission or competent UK authority (as applicable) has decided provides adequate protection for Personal Data (an "**adequacy finding**"); (ii) that has achieved binding corporate rules authorization in accordance with European Data Protection Law; or (iii) that has executed standard contractual clauses for transfers adopted or approved by the European Commission or the competent UK authority, as applicable.

5.1.3 The Parties agree that when the transfer of Personal Data from Company to Trend Micro is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows (which shall be incorporated into, and form part of, this Addendum).

- (a) In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:
  - (i) Module Two will apply to the extent that Company is a Controller of the Personal Data, and Module Three will apply to the extent that Company is a Processor of the Personal Data on behalf of a third party Controller;
  - (ii) in Clause 7, the optional docking clause will apply;
  - (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in clause 3.4 of this Addendum;
  - (iv) in Clause 11, the optional language will not apply;
  - (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;
  - (vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;
  - (vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the relevant information set out in the Agreement and Annex 1 to this Addendum; and
  - (viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this Addendum.

- (b) In relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:
- (i) for so long as it is lawfully permitted to rely on standard contractual clauses for the transfer of Personal Data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("**Prior C2P SCCs**") for transfers of Personal Data from the United Kingdom, the Prior C2P SCCs shall apply between the Company (which, where Company is a processor on behalf of a third party Controller, it enters on behalf of that Controller) and Trend Micro on the following basis:
    - (A) Appendix 1 shall be completed with the relevant information set out in the Agreement and Annex 1 to this Addendum;
    - (B) Appendix 2 shall be completed with the relevant information set out in Annex 2 to this Addendum; and
    - (C) the optional illustrative indemnification clause will not apply.
  - (ii) Where sub-paragraph **Error! Reference source not found.** above does not apply, but Company and Trend Micro are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the United Kingdom subject to completion of a "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:
    - (A) the EU SCCs, completed as set out above in sub-paragraph 5.1.3(a) shall also apply to transfers of such Personal Data, subject to sub-clause **Error! Reference source not found.** below; and
    - (B) the UK Addendum shall be deemed executed between the transferring Company and Trend Micro, and
      - i. the tables in Part 1 of the UK Addendum shall be deemed completed with the information set out in Annex 3 to this Addendum; and
      - ii. the EU SCCs shall be deemed amended as specified by Part 2 of the UK Addendum in respect of the transfer of such Personal Data.
  - (iii) If neither sub-paragraph **Error! Reference source not found.** or **Error! Reference source not found.** (ii) applies, then Company and Trend Micro shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay.
- (c) In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5.1.4 With respect to Personal Data protected by the EU GDPR, where any such Personal Data is transferred outside the European Economic Area to a territory not at that time subject to an adequacy finding recognised under the EU GDPR Trend Micro has entered into such standard contractual clauses for transfers of Personal Data from Trend Micro to its Affiliates outside the European Economic Area, in

relation to Trend Micro's Processing of such Personal Data as set out in this Addendum and the Agreement.

- 5.1.5 With respect to Personal Data protected by the UK GDPR, where any such Personal Data is transferred outside the UK to a territory not at that time subject to an adequacy finding recognised under the UK GDPR, Trend Micro has entered into such standard contractual clauses for transfers of Personal Data from Trend Micro to its Affiliates outside the United Kingdom, in relation to Trend Micro's Processing of such Personal Data as set out in this Addendum and the Agreement.
- 5.1.6 After Company has exercised its rights under clauses 3.103.10(a) and 3.103.10(b) above with respect to Personal Data protected by the UK GDPR or EU GDPR, if Company requires further information Company will have the right to, at its own cost and subject to Company's payment of Trend Micro's fees in relation to such audit at its standard professional services rates prevailing at the time, require that Trend Micro permit Company (or its independent third-party auditors) to carry out its own audit of Trend Micro's compliance with this Addendum, following which Trend Micro shall make available to Company all information, systems and staff necessary for Company (or its independent third-party auditors) to conduct such audit. If a third-party is to conduct the audit, the third-party must be mutually agreed to by Company and Trend Micro and must execute a written confidentiality agreement with Company and Trend Micro before conducting the audit. To request an audit, Company must submit a detailed audit plan at least 60 days in advance of the proposed audit date to Trend Micro describing the proposed scope, duration, and start date of the audit. Trend Micro will review the audit plan and provide Company with any concerns or questions (for example, any request for information that could compromise Trend Micro's security, privacy, employment or other relevant policies). Both Parties will work cooperatively in good faith to agree on a final audit plan. An audit must be conducted during normal business hours, and all reasonable measures must be taken to prevent unnecessary disruption to Trend Micro's operations. Company will not exercise such audit right more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent Regulator; or (ii) if Company believes a further audit is necessary due to a Security Incident suffered by Trend Micro.

## 5.2 **Applicable only to Switzerland Personal Data**

- 5.2.1 The following terms shall have the following meanings in this Clause 5.**Error! Reference source not found..**
- (a) "**Restricted Transfer**" means a transfer of Personal Data that is protected by the Swiss Federal Data Protection Act as amended from time to time ("**FDPA**") and the GDPR (where applicable) to a country outside of Switzerland which is not on the Swiss Federal Data Protection and Information Commissioner's ("**FDPIC**") list of countries that offers adequate protection ("**FDPIC List**"); and
- (b) "**Standard Contractual Clauses**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
- 5.2.2 Trend Micro shall not transfer any Personal Data outside of Switzerland to countries not on the FDPIC List, unless it has taken such measures as are necessary to ensure the transfer is in compliance with the FDPA and the GDPR (where applicable).
- 5.2.3 The Parties agree that when the transfer of Personal Data from Company to Trend Micro is a Restricted Transfer it shall be subject to the Standard Contractual Clauses as follows (which shall be incorporated into, and form part of, this Addendum).

- (a) In relation to Personal Data that is protected by the FDPA and GDPR (where applicable), the Standard Contractual Clauses will be adapted as follows ("**Swiss Adaptations**"):
- (i) *Supervisory Authority*: Insofar as the Personal Data transmission is only subject to the FDPA, the FDPIC is the exclusive supervisory authority. If the Personal Data transfer is subject to both the Swiss DPA and the GDPR, then a parallel supervision takes place: FDPIC, insofar as the Personal Data transfer is governed by the Swiss DPA; EU authority insofar as the Personal Data transfer is governed by the GDPR (the criteria of Clause 13a for the selection of the competent authority must be observed);
  - (ii) *Applicable law for contractual claims under Clause 17*: Swiss law or the law of a country that allows and grants rights as a third party beneficiary for contractual claims regarding Personal Data transfers pursuant to the FDPA; law of an EU member state for those according to the GDPR (free choice for Module 4);
  - (iii) *Place of jurisdiction for actions between the Parties pursuant to Clause 18 b*: If the Personal Data transfer is subject to the FDPA, the place of jurisdiction shall be at Trend Micro's domicile in Switzerland. If the Personal Data transfer is subject to the GDPR, then the court of an EU member state for actions concerning Personal Data transfers pursuant to the GDPR (free choice for Module 4) is the place of jurisdiction;
  - (iv) *Adjustments or additions concerning the place of jurisdiction for actions brought by Data Subjects*: The term "member state" must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c);
  - (v) *Adjustments or additions regarding references to the GDPR*: the references to the GDPR should be understood as references to the FDPA insofar as the Personal Data transfers are subject to the FDPA; and
  - (vi) *Supplement until the entry into force of the revised FDPA*: the clauses of the EU SCC also protect the Personal Data of legal entities until the entry into force of the revised FDPA.
- (b) In addition the Standard Contractual Clauses will apply completed as follows, unless already amended by the Swiss Adaptations:
- (i) Module Two will apply to the extent that Company is a Controller of the Personal Data, and Module Three will apply to the extent that Company is a Processor of the Personal Data on behalf of a third party Controller;
  - (ii) in Clause 7, the optional docking clause will apply;
  - (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 3.4 of this Addendum;
  - (iv) in Clause 11, the optional language will not apply;
  - (v) in Clause 17, Option 1 will apply, and the Standard Contractual Clauses will be governed by Swiss law;

- (vi) in Clause 18(b), disputes shall be resolved before the courts of at the domicile of Trend Micro in Switzerland;
- (vii) Annex I of the Standard Contractual Clauses shall be deemed completed with the relevant information set out in the Agreement and Annex 1 to this Addendum;
- (viii) Annex II of the Standard Contractual Clauses shall be deemed completed with the information set out in Annex 2 to this Addendum.

5.2.4 In the event that any provision of this Addendum contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5.2.5 With respect to Personal Data protected by the FDPA and GDPR (where applicable), where any such Personal Data is transferred outside of Switzerland to countries not on the FDPIC List, Trend Micro has entered into the Standard Contractual Clauses for transfers of such Personal Data from Trend Micro to its Affiliates outside of Switzerland, in relation to Trend Micro's Processing of such Personal Data as set out in this Addendum and the Agreement.

5.3 Trend Micro will comply with the Personal Data Protection Laws of other jurisdictions to the extent that Trend Micro Processes Personal Data that is subject to the Personal Data Protection Law of such other jurisdiction(s).

## **6. Liability**

6.1 For the avoidance of doubt, in no event shall the maximum aggregate liability of Trend Micro and all its Affiliates to Company and its Affiliates, including, without limitation, under the Agreement and (if applicable) any Standard Contractual Clauses previously entered into between Trend Micro or any of its Affiliates, on the one hand, and Company and/or any of its Affiliates, on the other, exceed the maximum liability as defined under the terms of the Agreement.

## **7. Governing law and jurisdiction**

7.1 This Addendum, the performance of the Parties hereunder, and all disputes arising out of or related hereto will be governed by and construed solely in accordance with the governing law provision of the Agreement, but giving due regard to any applicable Personal Data Protection Laws. The Parties irrevocably consent and agree to the sole and exclusive *in personam* jurisdiction of the courts (or arbitral tribunal as the case may be) as set forth in the Agreement with respect to any dispute that cannot be resolved by the Parties and all proceedings with respect thereto shall be litigated and determined solely and exclusively in such courts. Each of the Parties represents and agrees that such *in personam* jurisdiction is reasonable and fair and hereby waives any objection which it may now or hereafter have based on improper venue or forum non conveniens in such courts.

**Annex 1:**  
**Data Processing Description**

This Annex I forms part of the Addendum and describes the processing that the processor will perform on behalf of the controller.

**A. List of Parties**

**Controller / Data exporter:**

Name:	The name of Company as set out in the Agreement and/or the Licence Instrument.
Address:	The address of Company as set out in the Agreement and/or the Licence Instrument.
Contact person's name, position and contact details:	The contact person (and details thereof) for the signatory of Company as set out in the Agreement or as provided separately by the Company to Trend Micro.
Activities relevant to the data transferred under these Clauses:	Trend Micro's provision of Products and/or Services to Company under the Agreement, to the extent this involves Trend Micro Processing Personal Data on behalf of Company.
Signature and date:	As per the Agreement or as otherwise agreed between the Controller and the Data Importer/ Processor.
Role (controller/processor):	Company will be acting as controller and/or processor of Personal Data.

**Processor / Data importer:**

Name:	The name of Trend Micro as set out in the Agreement and/or Licence Instrument.
Address:	The address of Trend Micro as set out in the Agreement or as separately provided to Company by Trend Micro.
Contact person's name, position and contact details:	Lianne Harcup, Data Protection Officer – European DPO Department Contact: <a href="mailto:gdpr@trendmicro.com">gdpr@trendmicro.com</a> Globally the contact details are the same as above but will be distributed by the European DPO Department to the relevant Trend Micro Global entity.
Activities relevant to the data transferred under these Clauses:	Trend Micro offers a variety of data security products and services, including anti-virus, anti-malware and other software and cloud products. Trend Micro's provision of Products and/or Services to Company under the Agreement, to the extent this involves Trend Micro Processing Personal Data on behalf of Company.
Signature and date:	As per the Agreement or as otherwise agreed between the Data Importer/ Processor and the Controller.
Role (controller/processor):	Processor.

**B. Description of transfer**

<b>Purpose of the data transfer and further processing / Subject matter of Processing and processing operations</b>	Trend Micro offers a variety of data security products and services, including anti-virus, anti-malware and other software and cloud products. Trend Micro's provision of Products and/or Services to Company under the Agreement, to the extent this involves Trend Micro Processing Personal Data on behalf of Company.
<b>Duration of processing</b>	The term of the Agreement (plus any applicable exit period).
<b>Nature of the Processing</b>	The purpose of the Processing is Trend Micro's provision of Products and/or Services under the Agreement. The nature of the Processing may include (but is not limited to) collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

<b>Categories of Personal Data transferred</b>	Any Personal Data that Company decides to protect with Trend Micro Products and Services. The type of Personal Data that Company chooses to provide or make available to Trend Micro in the course of its use of Trend Micro's Products and/or Services under the Agreement, which may include (but is not limited to) IP addresses, URL strings, DNS data, email senders and recipients, contents of emails and attachments to emails, network telemetry data, files and various other unstructured or structured information (including information or data associated with any of the foregoing), which could include Personal Data.
<b>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:</b>	The Personal Data that may be Processed would not normally concern any special categories of Personal Data and Company is advised against providing Trend Micro with special categories of Personal Data or Personal Data relating to criminal convictions or offences.
<b>Categories of Data Subjects whose personal data is transferred</b>	Those Data Subjects whose Personal Data is provided or made available by Company to Trend Micro in the course of its use of Trend Micro's Products and/or Services under the Agreement. Data Subjects may include employees or customers of Company, at its sole discretion and control.
<b>Frequency of the transfer:</b>	Ongoing for the duration of Trend Micro's provision of the Products and/or Services.
<b>The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:</b>	Personal Data will be retained in accordance with Trend Micro's guidelines regarding the retention, storage, handling and disposal of records and information.
<b>For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:</b>	Where Trend Micro engages sub-processors it will do so in compliance with the terms of the applicable Standard Contractual Clauses. The subject matter, nature and duration of the processing activities carried out by any sub-processor will not exceed the subject matter, nature and duration of the processing activities as described in this Addendum.

### C. Competent supervisory authority

The competent supervisory authorities are:

- to the extent the Personal Data is protected by the EU GDPR, the supervisory authority of Ireland;
- to the extent the Personal Data is protected by the UK GDPR, the Information Commissioner; and
- insofar as the Swiss FDPA applies to the data transfers at issue, the Federal Data Protection and Information Commissioner (FDPIC).

Annex 2:  
Trend Micro Minimum Security Measures

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

*Description of the technical and organisational measures implemented by the Personal Data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

The measures described below (or similarly strong measures) are, to the greatest extent possible, imposed contractually as minimum security measures on any third party service providers used to process Personal Data.

<i>Measures of pseudonymisation and encryption of Personal Data</i>	<p>Deployment of end-point security solution including encryption and pseudonymization, along with high fidelity machine learning, behavioural analysis, exploit protection and advanced protection to against ransomware variants, file reputation, variant protection, browser exploit protection, web reputation (etc.) for threat and malware protection.</p> <p>Implementing appropriate controls to protect confidential and sensitive information from unauthorized disclosure and modification. Encryption must be applied to all information stored or transmitted as appropriate for the information classification and identified risks.</p> <p>Encryption key management is in place to support the use of cryptographic techniques.</p> <p>Encryption must be used for transmitting sensitive information where practicable.</p> <p>Full disk software encryption is enabled on the workstation operating system drives. Wireless access to the IT system is protected by encryption mechanisms.</p> <p>Pseudonymization measures include use of:</p> <ul style="list-style-type: none"><li>• Quasi-identifier</li><li>• Attribute suppression, particularly for sensitive Personal Data</li></ul> <p>Encryption measures include:</p> <ul style="list-style-type: none"><li>• HTTPS (TLS 1.2+) encryption for Personal Data transmission from Products to Trend Micro backend, using industry standard algorithms and certificates.</li></ul>
---	---

	<ul style="list-style-type: none"> <li>• Encryption of Personal Data at rest using the industry standard AES-256 algorithm with key rotations.</li> </ul>
<p><i>Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services</i></p>	<p>A secure internal web portal is utilised to authorize employees' access to the relevant Personal Data, including that hosted by external service providers. This includes the following measures:</p> <p><u>Confidentiality</u></p> <ul style="list-style-type: none"> <li>• Carrying out information classification to classify specific assets based on the relative sensitivity of the information they contain and providing guidelines for the treatment, disclosure and use of classified information.</li> <li>• Use of Virtual Private Network (VPN).</li> <li>• Secure transmission of credentials using TLS 1.2 (or greater).</li> <li>• Passwords require a defined minimum complexity. Initial passwords must be changed after the first login. Passwords must be changed at least on a quarterly basis and must be changed immediately if compromise is suspected.</li> <li>• There are internal guidelines for the handling of passwords.</li> <li>• Employees are subject to a non-disclosure agreement and all employees undergo a security awareness training course upon hire and on a yearly basis.</li> <li>• Access control: <ul style="list-style-type: none"> <li>• Maintaining access controls and policies to manage what access is allowed to each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Access to information assets is limited to Trend Micro employees and Trend Micro requires that this is used for business purposes only. Access to information assets may be granted to other individuals and entities upon explicit permission from Trend Micro management.</li> <li>• Users are provided with access to the network, services, applications and operating systems that have been specifically authorized by Trend Micro</li> </ul> </li> </ul>

	<p>management and on a 'need to know' basis.</p> <ul style="list-style-type: none"> <li>• Regular review of all access granted to users. Accounts are deleted when the user no longer requires access to the specific processing system.</li> <li>• Implementing suitable measures to ensure that Personal Data collected for different purposes can be processed separately. Personal Data is processed in a production network, separated from the internal network.</li> </ul> <p><u>Integrity</u></p> <ul style="list-style-type: none"> <li>• Use of firewalls to implement network access control; network Intrusion Detection System / Intrusion Prevention System (IDS/IPS) to protect against known, unknown, and undisclosed vulnerabilities; the secure web gateway for application control with zero-day exploit detection, advanced anti-malware scanning, real-time web reputation, and flexible URL filtering to provide superior internet threat protection.</li> <li>• Secure network interconnections ensured by firewalls etc.</li> <li>• Logging of transmissions of Personal Data from the IT system that stores or processes Personal Data.</li> <li>• Logging authentication and monitored logical system access and Personal Data access including, but not limited to, access, modification, entry and deletion of data.</li> <li>• Documentation of Personal Data entry rights and logging security related entries.</li> <li>• No possibility of deletion or modification of log files content by users. Access to the log files is logged in addition to monitoring for detecting unusual activity.</li> <li>• Implementing suitable measures to ensure that Personal Data are protected from accidental destruction or loss. Maintaining corrective action and incident response plans to respond to potential security threats.</li> </ul> <p><u>Availability</u></p> <ul style="list-style-type: none"> <li>• Information and software of all Trend Micro critical systems is backed-up and tested regularly, to ensure and maintain</li> </ul>
--	--

	<p>the integrity and availability of information and associated assets. Personal Data is backed up to multiple durable Personal Data stores and replicated across multiple availability zones.</p> <ul style="list-style-type: none"> <li>• Protection of stored backup media.</li> <li>• Establishment of business continuity plans to protect critical business processes and the associated assets from the effects of major interruption, failure or disasters.</li> <li>• Implementation of incident response and management processes, which include internal escalation requirements. If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication. Following an incident, the team examines the root cause, and revises the response plan accordingly.</li> </ul>
<p><i>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</i></p>	<ul style="list-style-type: none"> <li>• Upon the creation of any new service at Trend Micro, a team consisting of business and technical stakeholders is put together to create a business continuity plan containing backup, recovery and testing plans. These plans are approved by senior management and are tested at regular intervals.</li> <li>• Continuity Planning and Disaster Recovery Plans including: <ul style="list-style-type: none"> <li>○ Disaster recovery processes to restore Personal Data and processes</li> <li>○ Recovery Time Objective (RTO)</li> <li>○ Recovery Point Objective (RPO)</li> <li>○ Maximum Tolerable Downtime (MTD)</li> <li>○ Capacity management measures to monitor resource consumption of systems as well as planning of future resource requirements.</li> </ul> </li> <li>• Procedures for handling and reporting incidents (incident management) including the detection and reaction to possible security incidents.</li> <li>• Backups of Personal Data with near-real time replication. All backups are kept</li> </ul>

	<p>redundant and in encrypted form (AES-256).</p> <ul style="list-style-type: none"> <li>• See also further information provided under "<i>Measures for ensuring ongoing confidentiality...</i>" above.</li> </ul>
<p><i>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</i></p>	<ul style="list-style-type: none"> <li>• Establishment of a security organization, which has an objective to define security policies and rules for Trend Micro operations and monitor security effectiveness.</li> <li>• Information and security policy adherence and control effectiveness at Trend Micro is regularly checked through security audits and reviews by an independent party e.g. penetration tests. Trend Micro SaaS services are scanned with leading vulnerability scanning tools. When a vulnerability is found the account owners and the InfoSec team are notified automatically.</li> <li>• Where third party service providers are used to process Personal Data, they are contractually required to implement processes for regular testing, assessment and evaluation of security</li> <li>• Information is backed-up and tested regularly.</li> </ul>
<p><i>Measures for user identification and authorisation</i></p>	<ul style="list-style-type: none"> <li>• See information on access control under '<i>Measures for ensuring ongoing confidentiality...</i>' above.</li> <li>• Segregation of access control roles (e.g. access request, access authorization, access administration) is clearly defined and documented.</li> <li>• Logging of transmissions of Personal Data from IT system that stores or processes Personal Data.</li> <li>• Logging authentication and monitored system access.</li> <li>• All password activities are controlled through a formal process and Trend Micro requires that appropriate care be taken in allocation, distribution, reset and use of the passwords.</li> <li>• Remote access to Trend Micro's infrastructure is strictly controlled and monitored. All authentication methods used adhere to industry best practices/standards such as certificate-based and/or multi-factor authentication. Where appropriate, Single Sign-On (SSO)</li> </ul>

	leveraging the corporate directory is used.
<i>Measures for the protection of Personal Data during transmission</i>	<ul style="list-style-type: none"> <li>• Sensitive information must be transported through secure or controlled means.</li> <li>• Secure network interconnections ensured by VPN, MFA, firewalls etc.</li> <li>• Remote access to the network via VPN tunnel and end-to-end encryption.</li> <li>• HTTPS encryption for data in transit (using TLS 1.2 or greater), using industry standard algorithms and certificates.</li> <li>• Where third party service providers are used to process Personal Data, they are contractually required to implement access controls and other measures to protect access to their networks.</li> </ul>
<i>Measures for the protection of Personal Data during storage</i>	<ul style="list-style-type: none"> <li>• Implementation of suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the Personal Data media, including encryption and the use of firewalls or functionally equivalent technology to protect Personal Data.</li> <li>• Use of email security gateway to protect attack from email, detect the malicious URL and attachment in the email, block spam, phishing, and target attack.</li> <li>• Processes for the proper handling, storage and disposal of documents, computer media and systems documentation have been implemented.</li> <li>• All media containing sensitive or classified information is stored in a secure environment and in accordance with the manufacturer's specifications.</li> <li>• System documentation is stored securely.</li> <li>• System inputs are recorded via log files.</li> <li>• See information on access control under '<i>Measures for ensuring ongoing confidentiality...</i>' above.</li> </ul>
<i>Measures for ensuring physical security of locations at which Personal Data are processed</i>	<ul style="list-style-type: none"> <li>• Trend Micro accords a level of protection from physical security threats and environmental hazards commensurate with the associated risks for business information and information processing facilities.</li> </ul>

	<ul style="list-style-type: none"> <li>• Business information and information processing facilities supporting critical or sensitive business activities are housed in secure areas with appropriate entry controls. All access to Trend Micro offices and networks is strictly controlled and limited to authorized or accompanied users only. Further approval is required before entry is granted into sensitive areas.</li> <li>• Use of CCTV to deter, detect and analyse physical access intrusions.</li> <li>• All physical access by employees and contractors to Trend Micro facilities where physical components are housed is logged and routinely audited.</li> <li>• Where third party service providers are used to process Personal Data, they are contractually required to implement physical security measures to protect physical access to locations at which Personal Data are processed.</li> <li>• See further "Measures for the protection of Personal Data during storage".</li> </ul>
<i>Measures for ensuring events logging</i>	<p>Implementation of suitable measures to ensure that it is possible to check and establish whether and by whom Personal Data have been input into data Processing systems or removed.</p> <p>Maintaining audit logs of security events, and specifying minimum levels of information to be logged. Event logs are implemented and stored using management services.</p> <p>Implementation of suitable measures to monitor system administrators and to ensure that they act in accordance with instructions received.</p> <p>Logs are kept for an appropriate amount of time.</p> <p>Security logs are reviewed for all systems regularly by the Service Operations teams. Security event logs are also integrated with internal communication and alerting tools for real time oversight and event triage. If a security incident is suspected, it is immediately reported to the Trend Micro InfoSec team, where a formal incident response plan is executed. In addition, InfoSec monitors Trend Micro services environment logs.</p> <p>7x24 security operation team uses Central Security Event and Information Management (SIEM) system to collect logs (including the logs</p>

	from system, endpoint security products and network security products), and customized rules to correlate the logs to perform real-time monitor, analysis and response the security incident.
<i>Measures for ensuring system configuration, including default configuration</i>	<ul style="list-style-type: none"> <li>• See information on access control under '<i>Measures for ensuring ongoing confidentiality...</i>' above.</li> <li>• Certain configuration standards are required, including that all network components and services must be configured conforming to defined Trend Micro configuration standards.</li> <li>• Configuration Planning and Management.</li> <li>• Configuration Change Management.</li> <li>• Configuration Verification and Audits (changes are done through pull requests with reviews and approvals).</li> </ul>
<i>Measures for internal IT and IT security governance and management</i>	<p>Internal IT and IT security governance policies and procedures, designed to (a) satisfy security objectives, (b) identify reasonably foreseeable and internal risks to security, and (c) minimize security risks. An established "security management procedure" ensures information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken, and information security incidents are managed in a consistent and effective approach. A security organization has been established, which comprises members from top management. Security roles and responsibilities of members of the security organization and users are defined and documented in accordance with the information security policy. Assignment of roles and responsibilities for managing information, including an Information Manager for each function and segment. A dedicated Information Security (InfoSec) department. The InfoSec team works closely with the service operation teams and others on various aspects of security controls and training. Employees and contractors must pass security awareness training upon hire and regularly update knowledge.</p> <p>If security measures are adopted through external entities, obtaining a written description of the activities performed to help ensure compliance with security policies.</p>

<p><i>Measures for certification/assurance of processes and products</i></p>	<p>Trend Micro has ISO27001 certifications for most of its SaaS offerings, please see: <a href="https://www.trendmicro.com/en_us/about/trust-center/compliance.html">https://www.trendmicro.com/en_us/about/trust-center/compliance.html</a></p> <p>PCI DSS Level 1 (Cloud One)</p> <p>FIPS 140-2 (Deep Security, TippingPoint)</p> <p>Common Criteria EAL2+ (Deep Security, TippingPoint)</p> <p>SOC 2 Type II</p> <p>FIPS 140-2 (Deep Security, TippingPoint)</p> <p>Common Criteria EAL2+ (Deep Security, TippingPoint)</p>
<p><i>Measures for ensuring Personal Data minimisation</i></p>	<ul style="list-style-type: none"> <li>• The extent of Personal Data transmitted depends on how Company has configured its products, services, networks, and/or systems.</li> <li>• Any Personal Data received from or relating to employees or customers is deleted or pseudonymized as soon as possible.</li> <li>• Pseudonymization measures, see above.</li> <li>• See also below under 'Measures for ensuring limited Personal Data retention'.</li> <li>• In general, Trend Micro only collects the minimum data required for the purpose it is seeking to achieve.</li> </ul>
<p><i>Measures for ensuring Personal Data quality</i></p>	<ul style="list-style-type: none"> <li>• Measures to avoid unnecessary data duplication.</li> <li>• Quality assurance measures. Yearly review of the inventory of major information assets to ensure its accuracy. Regularly backing up and testing information and software of all Trend Micro critical systems to ensure and maintain the integrity and availability of information and associated assets.</li> </ul>
<p><i>Measures for ensuring limited Personal Data retention</i></p>	<ul style="list-style-type: none"> <li>• Guidelines regarding the retention, storage, handling and disposal of records and information.</li> <li>• Established retention schedule identifying essential record types and the period of time for which they must be retained.</li> <li>• Following termination, Company's Personal Data of which Trend Micro is a Processor will be deleted in accordance with the Data Processing Addendum.</li> </ul>

<p><i>Measures for ensuring accountability</i></p>	<ul style="list-style-type: none"> <li>• Top Trend Micro management is involved in the security organization.</li> <li>• Responsibility is assigned to ensure end-user privacy throughout the product lifecycle and through applicable business processes. Trend Micro management's responsibility for the Trend Micro's information security includes: <ul style="list-style-type: none"> <li>○ setting information security objectives;</li> <li>○ endorsing security strategy and direction;</li> <li>○ endorsing information security programs, policies and processes;</li> <li>○ ensuring appropriate level of resources available to the program;</li> <li>○ supporting information security policy formulation, enforcement, maintenance including reviews and changes.</li> </ul> </li> <li>• Personal Data privacy impact assessments are performed in accordance with applicable Personal Data Protection Law.</li> </ul>
<p><i>Measures for allowing Personal Data portability and ensuring erasure</i></p>	<ul style="list-style-type: none"> <li>• Certain Companies are able to login to retrieve certain Personal Data</li> <li>• Open formats (CSV and JSON) offered Company can export Personal Data.</li> <li>• Internal procedure for handling data deletion requests.</li> </ul>

### Annex 3

#### UK Addendum – Part 1: Tables

**Table 1: Parties**

<b>Start date</b>	The Effective Date			
<b>The Parties</b>	<b>Exporter (who sends the Restricted Transfer)</b>		<b>Importer (who receives the Restricted Transfer)</b>	
<b>Parties' details</b>	<b>Full legal name:</b>	The name of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	<b>Full legal name:</b>	The name of Trend Micro as set out in the Agreement and/ or Licence Instrument as provided by the Trend Micro.
	<b>Trading name (if different):</b>	The trading name of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	<b>Trading name (if different):</b>	N/A
	<b>Main address (if a company registered address):</b>	The address of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	<b>Main address (if a company registered address):</b>	The address of Trend Micro as set out in the Agreement and/ or Licence Instrument as provided by the Trend Micro.
	<b>Official registration number (if any) (company number or similar identifier):</b>	The company number of Company as set out in the Agreement and/ or Licence Instrument as provided by the Company.	<b>Official registration number (if any) (company number or similar identifier):</b>	The company number of Trend Micro as set out in the Agreement and/ or Licence Instrument as provided by the Trend Micro.
<b>Key Contact</b>	The contact person (and details thereof) for the signatory of Company as set out in the Agreement or as separately provided by the Company.		The contact person (and details thereof) for the signatory of Trend Micro as set out in the Agreement or as separately provided by the Trend Micro.	
<b>Signature</b>	As per the Agreement or as otherwise agreed between the Exporter and the Data Importer.		As per the Agreement or as otherwise agreed between the Importer and the Data Exporter.	

**Table 2: Selected SCCs, Modules and Selected Clauses**

<b>Addendum EU SCCs</b>			The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:			
<b>Module</b>	<b>Module in operation</b>	<b>Clause 7 (Docking clause)</b>	<b>Clause 11 (Option)</b>	<b>Clause 9a (Prior Authorisation or General Authorisation)</b>	<b>Clause 9a (Time period)</b>	<b>Is personal data received from the Importer combined with personal data collected by the Exporter?</b>
As selected in paragraph 5.1.3(a) of this Addendum.						Yes

**Table 3: Appendix Information**

The Appendix Information shall be deemed completed as set out in paragraph 5.1.3(a)(vii) and 5.1.3(a)(viii) of this Addendum.

**Table 4: Ending this Addendum when the Approved Addendum Changes**

<b>Ending this Addendum when the Approved Addendum changes</b>	Which Parties may end this Addendum as set out in Section 19: <ul style="list-style-type: none"><li>• Exporter</li><li>• Importer</li></ul>
--	---

## EXHIBIT B

### GLOBAL PRIVACY NOTICE

# TREND MICRO GLOBAL PRIVACY NOTICE FOR OUR WEBSITE AND PRODUCTS

(November 15, 2021)

Trend Micro Incorporated and its subsidiaries and affiliates (collectively, "**Trend Micro**" or "**we**") provides this Privacy Notice to help you understand the types of personal information that you provide to Trend Micro, what we do with that information and how we protect that information. We are committed to protecting your privacy and ensuring you have a positive experience on our websites ("**Website**") and in using the Trend Micro Products (which includes related services such as support) that our customers ("Customers") sign up for.

This Privacy Notice covers personal information we collect in connection with our:

1. [Websites](#) (**Part 1**)
2. [Products](#) (**Part 2**)
3. [Prospects](#) (**Part 3**)

## Contents

We've listed the contents of each Part of our Privacy Notice below. If you want more information on a particular section, just click on the link in the contents list to jump directly to of that section.

- Websites Part 1: Contents
  - A. What information is processed by Trend Micro when using our Websites and how is it used by Trend Micro?
  - B. Legal basis for processing (*EEA or UK only*)
  - C. Sharing personal information
  - D. Transfers over the internet to countries located outside the EEA or UK (*EEA/UK only*)
  - E. Data Retention
  - F. Protection and security of personal information
  - G. Managing Personal Information
  - H. Third-party websites
  - I. Communication preferences
  - J. EEA/UK data protection rights (*EEA/UK only*)
  - K. Controller (*EEA/UK only*)
  - L. Contact and Data Protection Officer
- Products/ Part 2: Contents
  - A. What information is processed by Trend Micro when using our Products and how is it used by Trend Micro?
  - B. Legal basis for processing (*EEA or UK only*)
  - C. Sharing personal information
  - D. Transfers over the internet to countries located outside the EEA or UK (*EEA/UK individuals only*)
  - E. Data Retention
  - F. Protection and security of personal information
  - G. Communication preferences
  - H. EEA/UK data protection rights (*EEA/UK only*)

- I. Controller (*EEA/UK only*)
- J. Contact and Data Protection Officer
- Prospects Part 3:Contents
  - A. What information is processed by Trend Micro, how is it used by Trend Micro and why?
  - B. Legal basis for processing (*EEA or UK only*)
  - C. Sharing personal information
  - D. Transfers over the internet to countries located outside the EEA or UK (*EEA/UK only*)
  - E. Data Retention
  - F. Protection and security of personal information
  - G. Communication preferences
  - H. EEA/UK data protection rights (*EEA/UK only*)
  - I. Controller (*EEA/UK only*)
  - J. Contact and Data Protection Officer

## • Changes to the Trend Micro Privacy Notice

This Privacy Notice was last updated on November 15, 2021. Trend Micro will occasionally update this Privacy Notice to reflect changes in our Products and Customer feedback. When we make changes to the Privacy Notice, we will revise the date at the top of the Privacy Notice. If there are material changes to this Privacy Notice or in how we will use your personal information or where we intend to further process your personal information for a purpose other than that for which the personal information were collected, we will notify either by prominently posting a notice of such changes prior to implementing the change or by directly sending you a notification.

### 1. PRIVACY FOR OUR WEBSITES

This Part 1 of the Notice covers the personal information collected regarding visitors to our Website. We identify below subsections that are only applicable for the European Economic Area ("**EEA**") or United Kingdom ("**UK**").

This Part 1 covers, in relation to our Websites:

- A. What information is processed by Trend Micro when using our Websites and how is it used by Trend Micro?
- B. Legal basis for processing (*EEA or UK only*)
- C. Sharing personal information
- D. Transfers over the internet to countries located outside the EEA (*EEA or UK only*)
- E. Data Retention
- F. Protection and security of personal information
- G. Managing Personal Information
- H. Third-party websites
- I. Communication preferences
- J. EEA/UK data protection rights (*EEA/UK only*)
- K. Controller (*EEA/UK only*)
- L. Contact and Data Protection Officer

#### a. What information is processed by Trend Micro when using our Websites and how is it used by Trend Micro?

## Information that is actively provided

Trend Micro collects personal information in many ways: when visitors download free evaluation software or upgrades, when visitors register online, when visitors contact Trend Micro through our “Contact Us” link on our Website, when visitors participate in a campaign or a website forum or referral promotions, when individuals register for or otherwise participate in a competition, when visitors request online a quote or technical support, when visitors cause information or data to be sent to Trend Micro as part of the Products, when visitors subscribe online to Trend Micro newsletters or receive Product updates or technical online alerts, when visitors enter an online contest, giveaway, promotion or special offer, when visitors provide us with feedback online, or when visitors apply for a job online with Trend Micro.

Where visitors visit our Websites and wish to download content, take part in a competition, purchase product or request information, visitors may be requested to provide details as follows:

- Name
- Phone number
- Email address
- Postal address
- Company name
- Billing and shipping information
- Other relevant information about visitors and visitors' systems and visitors' company
- Date of birth (only for certain competitions)
- Parent's or legal guardian's name and email address (only for certain competitions where participants are minors under a particular age (such as under 18 in Australia, under 17 in the United States, and Canada, under 20 in Japan (due to be under 18 from April 2022), and under 16 in parts of Europe) in accordance with applicable data protection law);

If visitors do not provide their personal information stated above to us, their use of those sections of our Websites could be restricted or impossible.

Trend Micro does neither wish to receive nor need any sensitive personal information, i.e. personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal information relating to criminal convictions or offences.

Where minors participate in competitions, we ask for the consent of their parent or legal guardian where they are under a certain age (varying based on their country) as set out above. Other than for such competitions, Trend Micro does not knowingly collect personal information from minors under the age of 16. If we learn that we have collected the personal information of a minor under the age of 16, Trend Micro will promptly delete such personal information.

## Information that is collected automatically

Trend Micro's Website, certain Products, interactive applications and email messages may use "cookies" and other technologies such as web beacons to collect certain information automatically from visitors' device. This may also include cookies placed by third parties in addition to Trend Micro. In some countries, including countries in the European Economic Area, this information may be considered personal information under applicable data protection laws.

The information we collect automatically may include information like visitors' IP address, device type, unique device identification numbers, browser-type, broad geographic location (e.g. country or city-level location) and other technical information. We may also collect information about how a visitor's device has interacted with our Website, including the pages accessed and links clicked.

Trend Micro also collects log files of traffic that visit our Website. These log files may include information such as a visitor's Internet Protocol (IP) address, browser information and language, domain name, date and time of request. We use this information to track aggregate traffic patterns throughout our websites. Trend Micro may collect and retain for a certain period IP address information of Customers in order to provide technical support, obtain geo-location information, for subscription and registration purposes and to secure our networks and systems. To the extent that IP addresses or similar identifiers are considered personal information by applicable data protection law, we treat these identifiers as personal information. Similarly, to the extent that non-personal information is combined with personal information, we treat the combined information as personal information for the purposes of our Privacy Notice.

For more information on the technologies used and to learn how to manage cookie preferences, please see Trend Micro's Website “Cookie Notice” at [trendmicro.com/cookie-notice](https://trendmicro.com/cookie-notice).

## How does Trend Micro use personal information?

Trend Micro Websites collect personal information to provide downloads of free evaluation software or upgrades, newsletters, respond to

requests for contact, downloads of whitepapers and to provide its Products and support to its Customers and allow a visitor to register.

We may further use and process personal information provided to us through our Websites such as by visitors completing contact or information request forms to provide visitors with new Product information or technical alerts and keep visitors informed about our Products, promotions and special offers.

Cookies and other tracking technologies are used on our Website and in our Products for a variety of reasons including to better understand visitor and Customer behaviour and improving our Products and advertising.

We also collect and process personal information for the following other purposes:

- Responding to or addressing requests, enquiries, complaints, feedback or opinion;
- Improving visitors' experience of our Website;
- Recording visitor preferences regarding their use of our Website;
- Communicating with or notifying of, or providing them with updates on Trend Micro Products or benefits available or technical news;
- Participating in competitions and awarding prizes;
- Evaluating a visitor's interest in employment in the case of employment applications submitted by them through our Website.

## **B. Legal basis for processing (EEA or UK only)**

We will only collect and process personal information of visitors to our Website if we have a lawful basis to do so, for reasons explained in this Notice. We may process information that we have collected for legal bases including:

- Where we process personal information for internal record keeping in accordance with tax and accounting requirements under applicable law, this processing is necessary for compliance with a legal obligation of Trend Micro.
- To access certain content on our website or receive services available through it, visitors may be required to set up an online account. The information collected and used by us at these points, is necessary to provide visitors the content or services. This processing of personal information is necessary for the performance of the contract between visitors and Trend Micro regarding such access or receipt.
- Where we use and process personal information visitors provided to us via Trend Micro Website to provide visitors with new Product information or technical alerts and to keep visitors informed about our Products, promotions and special offers, the processing of personal information for such direct marketing purposes is based either on consent or on legitimate interest grounds.
- Where a visitor is a Customer of Trend Micro and we need to respond to or address the visitor's requests, enquiries, complaints or feedback, processing is necessary for the performance of the contract between the visitor and Trend Micro.
- If visitors have requests, enquiries, complaints, feedback or provide an opinion and visitors are not a Customer of Trend Micro, processing is necessary for the purposes of the legitimate interests pursued by Trend Micro to address their communications to us.
- We rely on our legitimate interests where we process visitors' personal information to improve visitors' experiences on our Website and to improve and develop our Products.

- Where we process visitors' personal information to evaluate their interest in employment in the case of employment applications submitted by them, processing is necessary for the purposes of recruitment and in order to take steps at their request prior to entering into a potential employment contract.
- We may also need to carry out certain processing activities to comply with a legal obligation to which Trend Micro is subject.
- Where you enter a competition (on behalf of yourself or on behalf of a minor), the use of your personal information (or the relevant minor's personal information) is either (i) necessary for the performance of the contract (competition rules/terms and conditions) that you agree to or (ii) where applicable on the basis of your consent. It is the responsibility of the entrant to make sure that each participant (or their parent/legal guardian) is made aware and accepts the competition rules/terms and conditions and made aware of this and any competition specific privacy notice.
- Any involvement in market research will only be based on visitors' consent.

## c. Sharing personal information

Trend Micro is a global organization and may share personal information with its affiliated companies, distributors or partners in order to provide the high quality, localized Products or offers or competition services visitors have requested, meet their needs or provide visitors with Customer support. Trend Micro may engage contractors to provide certain services in connection with Products, such as providing technical support, handling order processing or shipping Products, marketing, hosting and conducting Customer research or satisfaction surveys.

For example, if visitors choose to purchase a license to a Trend Micro Product on our Website, visitors will be directed to the website of one of Trend Micro's e-commerce partner, such as Digital River, in order to purchase the license. Trend Micro and the pertinent e-commerce partner will need to share some personal information.

Trend Micro requires that all contractors keep personal information of our visitors secure and confidential and that they do not share such personal information with others or use it for their own marketing purposes.

It may be necessary by law, legal process, litigation and/or requests from public and governmental authorities within or outside visitors' country of residence for Trend Micro to disclose visitors' personal information. We may also disclose personal information about visitors if we determine that for purposes of national security, law enforcement or other issues of public importance, disclosure is necessary or appropriate.

Trend Micro may also disclose personal information if we determine that disclosure is necessary to enforce our terms and conditions or protect our Products or visitors. In addition, in the event of a reorganization, merger or sale, we may transfer any and all personal information we collect to the relevant third party.

## d. Transfers over the internet to countries located outside the EEA or UK (EEA/UK only)

Trend Micro is a global organisation, with affiliated legal entities, business processes, management structures, and technical systems that cross borders. We may process visitors' personal information outside the country in which visitors are located, including at data centers in the United States as well as other locations operated by Trend Micro, affiliates of Trend Micro or data processors engaged by Trend Micro. When we share visitors' personal information among Trend Micro affiliates globally, we will do this on the basis of Binding Corporate Rules or EU Standard Contractual Clauses available at [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

We may also transfer visitors' personal information to our contractors based in various countries in the world where we do business, who carry out data processing on behalf of Trend Micro. Some of these countries may provide less legal protection than others for visitors' personal information. However, in such cases the data transfer will be subject to appropriate safeguards, namely the EU Standard Contractual Clauses.

## e. Data retention

Trend Micro will keep visitors' personal information for as long as we have an ongoing legitimate business need to do so (for example, to provide a service a visitor has requested or to comply with applicable legal, tax or accounting requirements). When we have no ongoing legitimate business need to process visitors' personal information, we will either delete or anonymize it or, if this is not possible (for example,

because visitors' personal information has been stored in backup archives), then we will securely store that personal information until deletion is possible.

## f. Protection and security of personal information

As a global security leader, Trend Micro understands the importance of securing visitors' personal information. Trend Micro has taken appropriate security measures – including administrative, technical and physical measures - to maintain and protect visitors' personal information against loss, theft, misuse, unauthorized access, disclosure, alteration and destruction. Access to visitors' personal information is restricted to authorized personnel only.

## g. Managing own personal information

If visitors participate in a Trend Micro discussion forum or a Trend Micro competition that publishes entries online on our Website, visitors should be aware that the information visitors provide there will be made broadly available to others, and can be read (or watched), collected or used by other users of these forums/competition pages, inside or outside of Trend Micro. This information can be used to send individuals unsolicited messages. Visitors are responsible for the personal information visitors choose to submit in these instances. For example, if visitors list their name and email address in a forum posting, that information is public. Visitors should be careful and responsible when participating in any forum or discussion group or public competition on Trend Micro's Website and note that some of these forums or competitions may have additional rules and conditions. Each participant's opinion on a forum or competition in our Website is his or her own and should not be considered as reflecting the opinion of Trend Micro. Trend Micro is not responsible for the personal information or any other information visitors choose to submit in these forums or competitions.

Where visitors have a password which enables them to access their account, they are responsible for keeping this password secure and confidential.

## h. Third-party websites

Trend Micro's Website contains a number of links to websites of Trend Micro business partners or to co-branded websites that are maintained by Trend Micro and one or more of our business partners who are collecting visitors' personal information pursuant to their own policies and purposes. Visitors should carefully read the privacy policies on such websites or co-branded websites as they may differ from Trend Micro's Privacy Notice, especially as personal information collected on such websites are governed by the pertinent privacy policies. Trend Micro is not responsible for the content, their Products or privacy practices or misuse of any information visitors provide on those websites.

## i. Communication preferences

Trend Micro gives visitors the choice of receiving a variety of information that complements our Products. Visitors can manage their communication preferences and unsubscribe in one of the following ways:

- **Non-EEA/UK**

If visitors are based outside the EEA/UK: please email [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com) or send a letter to Trend Micro Privacy Program, Trend Micro Incorporated, c/o Legal Department, 225 East John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA. Visitors should include their name, email address and specific relevant information about the material that they no longer wish to receive.

- **EEA/UK**

If visitors are based in the EEA/UK: (a) Trend Micro promotional emails include instructions on how to unsubscribe from that particular communication; or (b) if visitors are an Enterprise Customer they may unsubscribe via our Preference Centre [https://resources.trendmicro.com/MyPreferenceCentre-en\\_GB.html](https://resources.trendmicro.com/MyPreferenceCentre-en_GB.html) or (c) if visitors are consumer customers they may unsubscribe via the "My Account" [https://www.trendsecure.com/my\\_account/signin/login](https://www.trendsecure.com/my_account/signin/login) or (d) unsubscribe by sending a message via email to [gdp@trendmicro.com](mailto:gdp@trendmicro.com) or via mail to Trend Micro EMEA Limited, c/o Data Protection Officer, Median House, IDA Business and Technology Park, Model Farm Road, Cork, Ireland. Visitors should include their name, email address and specific relevant information about the material that they no longer wish to receive.

## j. EEA/UK data protection rights (EEA/UK only)

Visitors to Trend Micro's European Website and visitors located in the EEA or UK have certain data protection rights under the General Data Protection Regulation of the European Union of 27 April 2016 ("GDPR") or the GDPR as it is saved and incorporated into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and "GDPR" is used to refer to either or both these laws). These are briefly explained below. If visitors wish to contact us in relation to those rights, please see the contact information at section 1.L below. We will endeavour to assist visitors where reasonably possible but please note that these rights may not apply in all circumstances and exceptions exist under the GDPR or applicable national law.

- **Right to rectification of personal information** - Visitors have the right to request that any inaccurate personal information held by or on behalf of Trend Micro is corrected.
- **Right to access personal information**– Visitors have the right to access their personal information held by Trend Micro. Please note that before we are able to respond to a request, we may ask visitors to verify their identity and to provide further details about their request. We will endeavour to respond without undue delay and, in any event, within the timescales required by law.
- **Right to data portability**– Visitors have the right to receive personal information they have provided to us or to ask us to transfer it to another company.
- **Right to erasure (or "right to be forgotten")**– Visitors have the right to request that Trend Micro delete all of the personal information that we hold about them.
- **Right to restrict processing**– Visitors have the right to restrict Trend Micro from processing their personal information, where: (1) they believe that the personal information held by us about them is not accurate; (2) they believe that the processing of their personal information is unlawful; (3) they believe that we no longer have any reason to process their personal information; or (4) they object to the processing as described below. In these circumstances we will restrict use of these visitors' personal information during the review period.
- **Right to object to processing**– Visitors have the right to ask Trend Micro to stop processing their personal information for direct marketing purposes or other purposes on grounds relating to their particular situation.
- **Right to withdraw consent** – If we are relying on visitors consent to use and process their personal information, they are free to withdraw that consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- **Right to make a complaint to a Data Protection Authority** - If visitors have a complaint or concerns about how we are processing their personal information or if they consider that the processing of their personal information by Trend Micro infringes the GDPR, then we will endeavor to address such concerns. However, if they would like to direct their complaint/concerns to a Data Protection Authority, they have such right under the GDPR.

If visitors have any questions, comments or concerns regarding this Privacy Notice or if visitors would like to change their communication preferences, update or review personal information we have about them or if visitors exercise a right to object, if visitors withdraw a consent they have given, or if visitors exercise any of their rights stated in this section, they can contact us using the EEA/UK contact information at section 1.L below. Visitors can also withdraw their consent or to object to processing of their personal information for direct marketing purposes by (for Enterprise Customers) visiting

Preference Centre [https://resources.trendmicro.com/MyPreferenceCentre-en\\_GB.html](https://resources.trendmicro.com/MyPreferenceCentre-en_GB.html), or our  
consumer customers) via their My Account: (for  
[https://www.trendsecure.com/my\\_account/signin/login](https://www.trendsecure.com/my_account/signin/login).

## κ. Controller [EEA/UK only]

Where the EU General Data Protection Regulation ("GDPR") or similar UK law applies, we must identify who the data controller is. When visitors are located inside the EEA or UK, Trend Micro EMEA Limited is the data controller of personal information that is collected through

their use of our Website.

## L. Contact and Data Protection Officer

- If visitors are based **outside the EEA/UK**, if they have any questions, requests, comments or concerns regarding this Privacy Notice, they can contact us using the details below:

Trend Micro Privacy Program Trend Micro  
Incorporated  
c/o Legal Department  
225 East John Carpenter Freeway Suite 1500  
Irving  
Texas 75062 USA  
E-Mail: [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)

- If visitors are based **inside the EEA or UK**, the contact details of the data protection officers designated by Trend Micro are:

### GDPR DPO:

Trend Micro (EMEA) Limited Lianne  
Harcup  
Median House  
IDA Business & Technology Park Model Farm  
Road  
Cork  
Ireland  
E-Mail: [gdpr@trendmicro.com](mailto:gdpr@trendmicro.com)

**For Trend Micro Deutschland GmbH:** HEC  
Harald Eul Consulting GmbH Harald Eul

Auf der Höhe 34 50321  
Brühl Deutschland  
E-Mail: [Datenschutz-TrendMicro@he-c.de](mailto:Datenschutz-TrendMicro@he-c.de)

## 2. PRIVACY FOR USERS OF OUR PRODUCTS

This Part 2 of the Notice covers the personal information of individuals (users) collected when signing up for or using Trend Micro's Products

- A. What information is processed by Trend Micro when using our Products and how is it used by Trend Micro?
- B. Legal basis for processing (*EEA/UK individual only*)
- C. Sharing personal information
- D. Transfers over the internet to countries located outside the EEA or UK (*EEA/UK individuals only*)
- E. Data Retention
- F. Protection and security of personal information
- G. Communication preferences
- H. EEA or UK data protection rights (*EEA/UK individual only*)
- I. Controller (*EEA/UK individual only*)
- J. Contact and Data Protection Officer

## A. What information is processed by Trend Micro when using our Products and how is it used by Trend Micro?

Upon ordering, purchasing, installing, activating or using our Products, we receive personal information such as:

- Name
- Phone number
- Email address
- Device ID
- Operating system
- License Key

We use this personal information to ensure that the relevant Customer's license to our solutions is valid and to contact our Customers regarding renewals, technical issues and new Product information.

The types of information and personal information that may be processed when using and interacting with our Products, including Customer support, include the following. The specific information and personal information that is processed will depend on the particular Product used.

These types of information and personal information enables users to participate, share and leverage Trend Micro's global database of threat related intelligence to rapidly identify and defend against potential threats within each Customer's unique network environment, as described in more detail below, as well as enabling us to provide any support requested. You can find further details of the types of data that Trend Micro products collect, what this data is used for and detailed instructions on how to disable the specific features that feedback data to Trend Micro in the Privacy and Personal Data Collection Disclosure. [LINK/URL: <https://success.trendmicro.com/data-collection-disclosure>]

- Product information, such as MAC address, device ID
- Public IP address of the user's gateway to the internet
- Mobile/PC environment
- Metadata from suspicious executable files
- URLs, Domains and IP addresses of websites visited and DNS data
- Metadata of user/device managed by gateway Product
- Application behaviours
- Personal information contained within email content or files to which Trend Micro is provided access
- Behaviours of Product users
- Information from suspicious email, including sender and receiver email address, and attachments
- Detected malicious file information including file name and file path
- Detected malicious network connection information
- Debug logs
- Network Architecture/Topology and network telemetry data
- Screen capture of errors
- Windows event log content
- WMI event content
- Registry data

Security and threat detection functions relating to our Products and functions includes:

- Analyse data sent to/from the user's device to isolate and identify threats, vulnerabilities, suspicious activity and attacks;
- Assess the reputation of a website, email sender's IP address, device or file to advise the user on whether access should be granted;
- Analyse email to protect against spam, impersonation and other suspicious content;

- Virus protection;
- Intrusion detection, prevention and protection;
- Threat prevention and prediction;
- Network defence;
- Sand box testing (for certain cloud products);
- Storage of emails for back up purposes (certain cloud products);
- Identify, block and/or remove applications, messages, and files that may compromise productivity or the performance and security of computers, systems, and/or networks;
- Identify sources and methods of targeted attacks; and
- Deliver updated protection against malicious threats.

We may also use personal information for other business purposes, including:

- Internal record keeping;
- Compliance with the law and requests from government bodies;
- Product development;
- Keeping existing and past Customers informed about our Products and promotions;
- Providing Customer support;
- Managing subscriptions and billing; and
- Responding to requests, questions and comments.

## Information that we obtain from third party sources

From time to time, we may receive personal information from third party sources such as distributors/ reseller or partners. The types of information we receive from these third parties includes contact information such as email addresses and telephone numbers and we use the information we receive from these third parties to contact individuals in relation to our products.

## B. Legal basis for processing (EEA/UK individuals only)

We will only collect and process user personal information if we have a lawful basis to do so, for reasons explained in this Notice.

### Products-related:

Many of our Products require an online account to be set up and purchases completed. The information collected and used by us at these points is necessary to provide the Products and support Customers expect from Trend Micro. In connection with Products, we may use personal information to renew or terminate a Customer's subscription or to complete a transaction or confirm or complete an order or offer. This processing of personal information is necessary for the conclusion and/or performance of the contract between the Customer and Trend Micro regarding the use of our Products and support and is in the Customer and Trend Micro's legitimate interests for the same reason.

We use and process personal information to ensure that the Customer's license to our solutions is valid and to contact Customers regarding renewals and contractual and technical issues. This processing is necessary for the performance of the contract between the Customer and Trend Micro regarding the use of our Products; and/or our legitimate interest in providing and improving our Products.

Where we use personal information provided through our Products to support Customers' network and information security, this processing is necessary for the performance of the contract between the Customer and Trend Micro and/or for the legitimate interest of the Customer in ensuring network and information security and our legitimate interest in providing and improving our Products.

### Direct Marketing:

Where we use and process personal information provided to us on account registration and/or Product purchase/installation/activation to provide our Customers with new Product information or technical alerts and to keep Customers informed about our Products, promotions and special offers, the processing of personal information for such direct marketing purposes is based either on consent or legitimate interest grounds.

## Other Purposes:

Where Trend Micro processes personal information for other purposes set out in this Privacy Notice, we rely on various legal bases:

- Where we process personal information for internal record keeping in accordance with tax and accounting requirements under applicable law, this processing is necessary for compliance with a legal obligation of Trend Micro.
- Where we need to respond to or address the requests, enquiries, complaints or feedback, processing is necessary for the performance of the contract between the relevant Customer and Trend Micro, our or their legitimate interests and/or is based on consent.
- We rely on our legitimate interests where we process personal information to provide, improve and develop our Products.
- We may also need to carry out certain other processing activities to comply with a legal obligation to which Trend Micro is subject.
- Any involvement in market research or beta programs will only be based on consent.

## c. Sharing personal information

Trend Micro is a global organization and may share personal information with its affiliated companies, resellers, distributors, vendors, service providers or partners in order to provide the high quality, localized Products or offers that Customers have requested, and/or to meet Customer needs or provide support. Trend Micro may engage contractors to provide certain services in connection with Products, such as providing technical support, hosting cloud services, handling order processing or shipping Products, conduct Customer research or satisfaction surveys. For example, if a Customer chooses to purchase a license to a Trend Micro Product on our Website, the Customer will be directed to the website of one of Trend Micro's e-commerce resellers, such as Digital River, in order to purchase the license. Trend Micro and the pertinent e-commerce reseller will need to share some personal information to complete the purchase.

Trend Micro requires that all contractors keep personal information of our Customers secure and confidential and that they do not share such personal information with others.

It may be necessary by law, legal process, litigation and/or requests from public and governmental authorities in any country, region or territory where Trend Micro operates, or from international or inter- governmental authorities or organisations, for Trend Micro to disclose personal information received in relation to the registration and/or use of our Products, in particular malicious or suspicious IP addresses, URLs, email addresses and/or domain names. We may also disclose such personal information if we determine that, for purposes of national security, law enforcement or other issues of national, regional or international public importance, disclosure is necessary or appropriate.

Trend Micro may also disclose personal information if we determine that disclosure is necessary to enforce our terms and conditions or protect our Products or their users. In addition, in the event of a reorganization, merger or sale, we may disclose and transfer any and all personal information we collect to the relevant third party.

## d. Transfers over the internet to countries located outside the EEA or UK (EEA/UK individuals only)

Trend Micro is a global organisation, with affiliated legal entities, business processes, management structures, and technical systems that cross borders. We may process user's personal information outside the country in which they are located, including at data centers in the United States as well as other locations operated by Trend Micro, affiliates of Trend Micro or data processors engaged by Trend Micro. When we share personal information among Trend Micro affiliates globally, we will do this on the basis of Binding Corporate Rules or EU Standard Contractual Clauses available at [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en).

We may also transfer personal information to our contractors based in various countries in the world where we do business, who carry out data processing on behalf of Trend Micro. Some of these countries may provide less legal protection than others for personal information. However, in such case the data transfer will be subject to appropriate safeguards, namely the EU Standard Contractual Clauses.

## e. Data retention

Trend Micro will keep personal information relating to the registration and use of our Products for as long as the relevant Customer remains a registered subscriber or for as long as we have another legitimate business purpose to do so and, thereafter, for no longer than is required or permitted by law. When we have no ongoing legitimate business need to process such personal information, we will either delete or anonymize it or, if this is not possible (for example, because the personal information has been stored in backup archives), then we will securely store the personal information until deletion is possible.

## f. Protection and security of personal information

As a global security leader, Trend Micro understands the importance of securing personal information. Trend Micro has taken appropriate security measures – including administrative, technical and physical measures - to maintain and protect personal information against loss, theft, misuse, unauthorized access, disclosure, alteration and destruction. Access to personal information relating to the registration and use of our Products is restricted to authorized personnel only.

Where a Customer has a password to enable access to the Customer's account, the Customer is responsible for keeping this password secure and confidential.

## g. Communication preferences

Trend Micro gives individuals the choice of receiving a variety of information that complements our Products. Communication preferences can be managed, including terminating subscriptions or future communications, in one of the following ways:

- **Non-EEA/UK**

Individuals based outside the EEA/UK: please email [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com) or send a letter to Trend Micro Privacy Program, Trend Micro Inc., c/o Legal Department, 225 East John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA. Please include the name, email address and specific relevant information about the material which should no longer be sent out.

- **EEA/UK**

Individuals based in the EEA/UK: (a) Trend Micro promotional emails include instructions on how to unsubscribe from that particular communication; or (b) for enterprise customers unsubscribe via our Preference Centre [https://resources.trendmicro.com/MyPreferenceCentre-en\\_GB.html](https://resources.trendmicro.com/MyPreferenceCentre-en_GB.html) or (c) for consumer customers unsubscribe via the "My Account" [https://www.trendsecure.com/my\\_account/signin/login](https://www.trendsecure.com/my_account/signin/login) or (d) unsubscribe by sending a message via email to [gdpr@trendmicro.com](mailto:gdpr@trendmicro.com) or via mail to Trend Micro EMEA Limited, c/o Data

## h. EEA/UK data protection rights (EEA/UK individuals only)

Individuals in the EEA/UK, under the General Data Protection Regulation of the European Union of 27 April 2016 ("GDPR") or the GDPR as it is saved and incorporated into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and "GDPR" is used to refer to either or both these laws) have certain data protection rights. These are briefly explained below. To contact us in relation to those rights, please see the contact information in section 2.J below. We will endeavour to assist where reasonably possible but please note that these rights may not apply in all circumstances and exceptions exist under the GDPR or applicable national law.

- **Right to rectification of personal information** - EEA/UK individuals have the right to request that any inaccurate personal information about them held by or on behalf of Trend Micro is corrected.
- **Right to access personal information** – EEA/UK individuals have the right to access their personal information held by Trend Micro. Please note that before we are able to respond to a request, we may ask to verify the requestor's identity and for further details about the request. We will endeavour to respond without undue delay and, in any event, within the timescales required by law.
- **Right to data portability** – EEA/UK individuals have the right to receive personal information they have provided to us or to ask us to transfer it to another company.
- **Right to erasure (or "right to be forgotten")** – EEA/UK individuals have the right to request that Trend Micro delete all of the personal information that we hold about them.
- **Right to restrict processing** – EEA/UK individuals have the right to restrict Trend Micro from processing their personal information, where: (1) they believe that the personal information held by us about them is not accurate; (2) they believe that the processing of their personal information is unlawful; (3) they believe that we no longer have any reason to process their personal information; or (4) they object to the processing as described below. In these circumstances we will restrict use of the requestor's personal information during the review period.
- **Right to object to processing** – EEA/UK individuals have the right to ask Trend Micro to stop processing their personal information for direct marketing purposes or other purposes on grounds relating to their particular situation.
- **Right to withdraw consent** – If we are relying on EEA/UK individuals' consent to use and process their personal information, they are free to withdraw that consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- **Right to make a complaint to a Data Protection Authority** - If EEA/UK individuals have a complaint or concerns about how we are processing their personal information or if they consider that the processing of their personal information by Trend Micro infringes the GDPR, then we will endeavor to address such concerns. However, if they would like to direct their complaint/concerns to a Data Protection Authority, they have such right under the GDPR.

If EEA/UK individuals have any questions, comments or concerns regarding this Privacy Notice or would like to change their communication preferences, update or review personal information we have about them or if they exercise a right to object, if they withdraw a consent they have given, or if they exercise any of the rights stated in this section, please contact us using the EEA/UK contact information in section 2.J below. Enterprise Users can also withdraw their consent or to object to processing of their personal information for direct marketing purposes by visiting our Preference Centre [https://resources.trendmicro.com/MyPreferenceCentre-en\\_GB.html](https://resources.trendmicro.com/MyPreferenceCentre-en_GB.html) or Consumers via their My Account: [https://www.trendsecure.com/my\\_account/signin/login](https://www.trendsecure.com/my_account/signin/login).

## i. Controller (EEA/UK individuals only)

Trend Micro Ireland Limited, Median House, IDA Business and Technology Park, Model Farm Road, Cork, Ireland is the data controller of personal information that is collected through use of our Products signed up for by EEA/UK Customers.

## j. Contact and Data Protection Officer

- Individuals based **outside the EEA/UK**, with any questions, requests, comments or concerns regarding this Privacy Notice, can contact us using the details below:

Trend Micro Privacy Program Trend  
Micro Incorporated  
c/o Legal Department  
225 East John Carpenter Freeway Suite 1500  
Irving Texas  
75062 USA  
E-Mail: [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)

- For individuals based **inside the EEA/UK**, the contact details of the data protection officers designated by Trend Micro are:

### GDPR DPO:

Trend Micro (EMEA) Limited Lianne  
Harcup  
Median House  
IDA Business & Technology Park Model  
Farm Road  
Cork  
Ireland  
E-Mail: [gdpr@trendmicro.com](mailto:gdpr@trendmicro.com)

**For Trend Micro Deutschland GmbH:** HEC  
Harald Eul Consulting GmbH Harald Eul

Auf der Höhe 34  
50321 Brühl  
Deutschland  
E-Mail: [Datenschutz-TrendMicro@he-c.de](mailto:Datenschutz-TrendMicro@he-c.de)

### 3. PRIVACY IN RELATION TO PROSPECTS

This Part 3 of the Notice covers the personal information collected regarding individuals who attend events, individuals who provide us with their business contact information, individuals who contact us with enquiries and other individuals that we send marketing to ("Prospects"). We identify below subsections that are only applicable for the European Economic Area ("EEA") or United Kingdom ("UK").

This Part 3 covers, in relation to Prospects:

- A. What information of Prospects is processed by Trend Micro, how is it used by Trend Micro and why?
- B. Legal basis for processing (*EEA/UK only*)
- C. Sharing personal information
- D. Transfers over the internet to countries located outside the EEA or UK (*EEA/UK only*)
- E. Data Retention
- F. Protection and security of personal information
- G. Communication preferences
- H. EEA/UK data protection rights (*EEA/UK only*)
- I. Controller (*EEA/UK only*)
- J. Contact and Data Protection Officer

#### A. What information is processed by Trend Micro, how is it used by Trend Micro and why?

##### Information that is actively provided

Trend Micro collects personal information in many ways, such as when Prospects: register to attend one of our events, provide us with their business card information or when they request to receive information from us.

The personal information can include:

- Contact details including name, telephone numbers, email address and postal address;
- Where relevant employer and employment information such as job title, function, seniority, department, and the address/country/city of the individual's office; and
- Contact's preferences and interests, for instance which newsletters they would like to be subscribed to or what products they are interested in.

Trend Micro collects this information in order to:

- respond to correspondence and enquiries Prospects send us;
- to provide events and other services requested by Prospects or their employer;
- obtain Prospects' feedback;
- send Prospects tailored information on our Products that may be of interest to them; and
- tailor and develop our Products to ensure they are as relevant as possible.

Trend Micro does neither wish to receive nor need any sensitive personal information, i.e. personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal information relating to criminal convictions or offences.

Trend Micro does not knowingly collect personal information from children under the age of 16. If we

learn that we have collected the personal information of a child under the age of 16, Trend Micro will promptly delete such personal information.

## Information that is collected automatically

Trend Micro's email messages may use technologies such as web beacons to collect certain information automatically from individuals' devices. In some countries, including countries in the European Economic Area, this information may be considered personal information under applicable data protection laws.

The information we collect automatically may include information like individuals' IP address, device type, unique device identification numbers, browser-type, broad geographic location (e.g. country or city-level location) and other technical information.

To the extent that IP addresses or similar identifiers are considered personal information by applicable data protection law, we treat these identifiers as personal information. Similarly, to the extent that non- personal information is combined with personal information, we treat the combined information as personal information for the purposes of our Privacy Notice.

For more information on the technologies used and to learn how to manage cookie preferences, please see Trend Micro's "Cookie Notice" at [trendmicro.com/cookie-notice](https://trendmicro.com/cookie-notice).

## Information that we obtain from third party sources

From time to time, we may receive personal information from third party sources such as lead generating companies, event hosting companies and employers of individuals who for example, wish their employees/ individuals to attend our events.

The types of information we receive from third parties include: name, email address, contact details (and where appropriate employment details). We use the information we receive from these third parties for lead generation/ marketing purposes, to enable us to send Prospects tailored information on our Products (including events) that may be of interest to them and to tailor and develop our Products .

## B. Legal basis for processing (EEA/UK only)

We will only collect and process personal information of Prospects if we have a lawful basis to do so, for reasons explained in this Notice. We may process information that we have collected for legal bases including:

- Where we process personal information for internal record keeping in accordance with tax and accounting requirements under applicable law, this processing is necessary for compliance with a legal obligation of Trend Micro.
- Information collected to enable Prospects to attend our events is necessary for the performance of the contract between such Prospects and Trend Micro for the provision of the event; or for the legitimate interests of Trend Micro and the employers of Prospects, where Prospects attend events on their employer's behalf.
- Where we use and process personal information to provide Prospects with new Product information or technical alerts and to keep them informed about our Products, promotions and special offers, the processing of personal information for such direct marketing purposes is based either on consent or on legitimate interest grounds.

- If Prospects have requests, enquiries, complaints, feedback or provide an opinion and are not a Customer of Trend Micro, processing is necessary for the purposes of the legitimate interests pursued by Trend Micro to address their communications to us.
- We rely on our legitimate interests where we process Prospects' personal information to improve their experiences of our events, to request feedback and/or to improve and develop our Products.
- We may also need to carry out certain processing activities to comply with a legal obligation to which Trend Micro is subject.
- The award of prizes and any involvement in market research will only be based on Prospects' consent.

## c. Sharing personal information

Trend Micro is a global organization and may share personal information with its affiliated companies, distributors, vendors or partners in order to provide the high quality, localized Products or offers Prospects have requested, meet their needs or provide Prospects with support. Trend Micro may engage contractors to provide certain services, such as providing technical support, marketing, and conducting research or satisfaction surveys.

Trend Micro requires that all contractors keep personal information of Prospects secure and confidential and that they do not share such personal information with others or use it for their own marketing purposes.

It may be necessary by law, legal process, litigation and/or requests from public and governmental authorities within or outside Prospects' country of residence for Trend Micro to disclose Prospects' personal information. We may also disclose personal information about Prospects if we determine that for purposes of national security, law enforcement or other issues of public importance, disclosure is necessary or appropriate.

Trend Micro may also disclose personal information if we determine that disclosure is necessary to enforce our terms and conditions or protect our Products or Prospects. In addition, in the event of a reorganization, merger or sale, we may transfer any and all personal information we collect to the relevant third party.

## d. Transfers over the internet to countries located outside the EEA/UK (EEA/UK only)

Trend Micro is a global organisation, with affiliated legal entities, business processes, management structures, and technical systems that cross borders. We may process Prospects' personal information outside the country in which Prospects are located, including at data centers in the United States as well as other locations operated by Trend Micro, affiliates of Trend Micro or data processors engaged by Trend Micro. When we share Prospects' personal information among Trend Micro affiliates globally, we will do this on the basis of Binding Corporate RulesEU Standard Contractual Clauses available at [https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

We may also transfer Prospects' personal information to our contractors based in various countries in the world where we do business, who carry out data processing on behalf of Trend Micro. Some of these countries may provide less legal protection than others for Prospects' personal information. However, in such case the data transfer will be subject to appropriate safeguards, namely the EU Standard Contractual Clauses.

## e. Data retention

Trend Micro will keep Prospects' personal information for as long as we have an ongoing legitimate business need to do so (for example, to provide a service or information that Prospects have requested or to comply with applicable legal, tax or accounting requirements). When we have no ongoing legitimate business need to process Prospects' personal information, we will either delete or anonymize it or, if this is not possible (for example, because Prospects' personal information has been stored in backup archives), then we will securely store that personal information until deletion is possible.

## f. Protection and security of personal information

As a global security leader, Trend Micro understands the importance of securing Prospects' personal information. Trend Micro has taken appropriate security measures – including administrative, technical and physical measures - to maintain and protect Prospects' personal information against loss, theft, misuse, unauthorized access, disclosure, alteration and destruction. Access to Prospects' personal information is restricted to authorized personnel only.

## g. Communication preferences

Trend Micro gives individuals the choice of receiving a variety of information about our Products. Individuals can manage their communication preferences and unsubscribe in one of the following ways:

- **Non-EEA/UK**

If Individuals are based outside the EEA/UK: please email [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com) or send a letter to Trend Micro Privacy Program, Trend Micro Inc, c/o Legal Department, 225 East John Carpenter Freeway, Suite 1500, Irving, TX 75062, USA. Individuals should include their name, email address and specific relevant information about the material that they no longer wish to receive.

- **EEA/UK**

If Prospects are based in the EEA/UK: (a) Trend Micro promotional emails include instructions on how to unsubscribe from that particular communication; or (b) sending a message via email to [gdpr@trendmicro.com](mailto:gdpr@trendmicro.com) or via mail to Trend Micro EMEA Limited, c/o Data Protection Officer, Median House, IDA Business and Technology Park, Model Farm Road, Cork, Ireland. Prospects should include their name, email address and specific relevant information about the material that they no longer wish to receive.

## h. EEA/UK data protection rights (EEA/UK only)

Prospects located in the EEA/UK have certain data protection rights under the General Data Protection Regulation of the European Union of 27 April 2016 ("GDPR") or the GDPR as it is saved and incorporated into UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and "GDPR" is used to refer to either or both these laws). These are briefly explained below. If Prospects wish to contact us in relation to those rights, please see the contact information at section 3.J below. We will endeavour to assist Prospects where reasonably possible but please note that these rights may not apply in all circumstances and exceptions exist under the GDPR or applicable national law.

- **Right to rectification of personal information** – Prospects have the right to request that any inaccurate personal information held by or on behalf of Trend Micro is corrected.
- **Right to access personal information** – Prospects have the right to access their personal information held by Trend Micro. Please note that before we are able to respond to a request, we may ask Prospects to verify their identity and to provide further details about their request.

We will endeavour to respond without undue delay and, in any event, within the timescales required by law.

- **Right to data portability** – Prospects have the right to receive personal information they have provided to us or to ask us to transfer it to another company.
- **Right to erasure (or "right to be forgotten")** – Prospects have the right to request that Trend Micro delete all of the personal information that we hold about them.
- **Right to restrict processing** – Prospects have the right to restrict Prospects from processing their personal information, where: (1) they believe that the personal information held by us about them is not accurate; (2) they believe that the processing of their personal information is unlawful; (3) they believe that we no longer have any reason to process their personal information; or (4) they object to the processing as described below. In these circumstances we will restrict use of these Prospects' personal information during the review period.
- **Right to object to processing** – Prospects have the right to ask Trend Micro to stop processing their personal information for direct marketing purposes or other purposes on grounds relating to their particular situation.
- **Right to withdraw consent** – If we are relying on Prospects' consent to use and process their personal information, they are free to withdraw that consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- **Right to make a complaint to a Data Protection Authority** – If Prospects have a complaint or concerns about how we are processing their personal information or if they consider that the processing of their personal information by Trend Micro infringes the GDPR, then we will endeavor to address such concerns. However, if they would like to direct their complaint/concerns to a Data Protection Authority, they have such right under the GDPR.

If Prospects have any questions, comments or concerns regarding this Privacy Notice or if Prospects would like to change their communication preferences, update or review personal information we have about them or if Prospects exercise a right to object, if Prospects withdraw a consent they have given, or if Prospects exercise any of their rights stated in this section, they can contact us using the EEA/UK contact information at section 3.J below.

#### **I. Controller (EEA/UK only)**

Where the EU General Data Protection Regulation ("GDPR") or similar UK applies, we must identify who the data controller is. Where Prospects' personal information is collected for Trend Micro EMEA Limited's purposes, Trend Micro EMEA Limited is the data controller of Prospects' personal information.

## **J. Contact and Data Protection Officer**

- If Prospects are based **outside the EEA/UK**, if they have any questions, requests, comments or concerns regarding this Privacy Notice, they can contact us using the details below:

Trend Micro Privacy Program Trend  
Micro Incorporated  
c/o Legal Department  
225 East John Carpenter Freeway Suite 1500  
Irving



Securing Your  
Connected World

Texas 75062 USA

E-Mail: [legal\\_notice@trendmicro.com](mailto:legal_notice@trendmicro.com)

- If Prospects are based **inside the EEA/UK**, the contact details of the data protection officers designated by Trend Micro are:

## GDPR DPO:

Trend Micro (EMEA) Limited Lianne

Harcup

Median House

IDA Business & Technology Park Model Farm

Road

Cork Ireland

E-Mail: [gdpr@trendmicro.com](mailto:gdpr@trendmicro.com)

**For Trend Micro Deutschland GmbH:** HEC

Harald Eul Consulting GmbH Harald Eul

Auf der Höhe 34 50321

Brühl Deutschland

E-Mail: [Datenschutz-TrendMicro@he-c.de](mailto:Datenschutz-TrendMicro@he-c.de)

## EXHIBIT C BUSINESS ASSOCIATE AGREEMENT

### HIPAA BUSINESS ASSOCIATE AGREEMENT

This **HIPAA Business Associate Agreement** (the “**BAA**”) is an addendum to each Trend published template such as a cloud service terms of service/use, enterprise software license agreement, technical or premium services or support agreement, and/or statement of work that specifically incorporates therein this BAA by reference hereto (each referred to herein as, the “**Agreement**”) between Trend Micro Incorporated, a California corporation or an Affiliate thereof (each referred to herein as “**Trend Micro**”) and Company. Each of Company and Trend Micro is a “**Party**” hereto and are sometimes referred to collectively herein as “**Parties**.” This BAA is made a part of and subject to the Agreement for all purposes, but in the event of conflict between this BAA and the Agreement, this BAA will control. This BAA replaces any earlier business associate agreement between the Parties with respect to the subject matter hereof and the Agreement.

#### 1. APPLICABILITY; DEFINITIONS.

**1.1 Applicability.** With respect to Trend Micro Products to be provided under the Agreement, this BAA shall be applicable only if and to the extent that Company is a Covered Entity or a Business Associate under HIPAA that makes available Protected Health Information as a part of Company Data it provides and or otherwise makes available to Trend Micro under the Agreement and Trend Micro otherwise meets the definition of a Business Associate under HIPAA with respect to such Protected Health Information.

**1.2 Definitions.** Except as otherwise defined in this BAA, capitalized terms shall have the definitions given them in HIPAA and are incorporated herein by reference such as, for example: Use, Disclosure, Designated Record Set, Breach, Security Incident, and Subcontractor, and if not defined by HIPAA, such terms shall have the definitions set forth in the Agreement. Specific Definitions:

“**Breach Notification Rule**” means the Breach Notification for Unsecured Protected Health Information as set forth at 45 CFR § 164 subpart D.

“**Business Associate**” shall have the same meaning as the term “business associate” in 45 CFR § 160.103.

“**CFR**” shall mean the Code of Federal Regulations referencing specific HIPAA provisions.

“**Company**” for this BAA only, means Company.

“**Covered Entity**” or “**CE**” shall have the same meaning as the term “covered entity” in 45 CFR § 160.103.

“**HIPAA**” collectively means the administrative simplification provision of the Health Insurance Portability and Accountability Act enacted by the United States Congress, and its implementing regulations, including the Privacy Rule, the Breach Notification Rule, and the Security Rule, as amended from time to time, including by the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”) and future modifications or amendments to any of the foregoing.

“**Privacy Rule**” means the Standards for Privacy of Individually Identifiable Health Information set out in the regulations at 45 CFR §§ 160 and 164, subparts A and E.

“**Protected Health Information**” or “**PHI**” shall have the same meaning as the term “protected health information” in 45 CFR § 160.103 including any electronic Protected Health Information (ePHI) as defined in the Privacy Rules, provided that it is limited to such ePHI that is received by Trend Micro from, or created, received, maintained, or transmitted by Trend Micro on behalf of, Company: (a) through the Use of any Trend Micro Product by Company, or (b) through Trend Micro’s performance of any managed service or support service under the Agreement.

“**Security Rule**” means the Security Standards for the Protection of Electronic Protected Health Information, set forth at 45 CFR §§ 160 and 164 subparts A and C.

“**Trend Micro Product(s)**” means any application software, hardware-based appliance, cloud service or managed service offered by Trend Micro and support provided with respect thereto under the Agreement from time-to-time while this BAA is in effect. Trend Micro Product(s) does not include any product licensed under Trend Micro End User License Agreement

“**Unsuccessful Security Incidents**” means, without limitation, pings and other broadcast attacks on Trend Micro’s firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, as long as no such incident results in unauthorized access, acquisition, Use, or Disclosure of Protected Health Information.

## **2. RESPONSIBILITIES OF TREND MICRO WITH RESPECT TO PHI.**

**2.1 Limitations on Use and Disclosure.** Trend Micro shall not Use and/or Disclose the Protected Health Information other than as permitted or required by this BAA and/or as otherwise Required by Law. Trend Micro shall make reasonable efforts to Use, Disclose, and/or request the minimum necessary Protected Health Information to accomplish the intended purpose of such Use, Disclosure, or request. Trend Micro shall not violate the HIPAA prohibition on the sale of Protected Health Information.

**2.2 Safeguards.** Trend Micro shall: (a) utilize appropriate safeguards to prevent the Use and Disclosure of Protected Health Information other than as provided for in this BAA; and (b) comply with the applicable requirements of the Security Rule with respect to the electronic Protected Health Information. Trend Micro will implement and will maintain appropriate administrative, physical and technical safeguards (including written policies and procedures) to prevent the unauthorized Use or Disclosure of electronic PHI that it creates, receives, maintains, or transmits on behalf of Company as required by the Security Rule and the HITECH Act.

**2.3 Reporting.** Trend Micro shall report to Company, without unreasonable delay, but in no event more than five (5) business days of discovery: (1) any Use and/or Disclosure of Protected Health Information that is not permitted or required by this BAA of which Trend Micro becomes aware; (2) any Security Incident of which it becomes aware, but for the avoidance of doubt, reporting of Unsuccessful Security Incidents shall not be required hereunder unless reporting is specifically required by Trend Micro Services purchased in the Agreement; and/or (3) any Breach of Company’s Unsecured Protected Health Information that Trend Micro may discover in accordance the Breach Notification Rule, see further 45 CFR §§ 164.404(c)(2) and 410. Trend Micro shall cooperate with Company in investigating any Breach and in meeting Company’s obligations under HIPAA. Taking into account the level of risk reasonably likely to be presented by the Use, Disclosure, Security Incident, or Breach, the timing of other reporting to third parties will be made consistent with Trend Micro’s and Company’s legal obligations. Notification(s) under this Section, if any, will be delivered to contacts identified by Company from time-to-time by any means Trend Micro selects, including through e-mail, and shall include the following information: (a) a brief description of what occurred, the date of the breach and the date of discovery of the Breach, if known; (b) a description of the type of Unsecured Protected Health Information involved; (c) identification, if known, of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Trend Micro, to have been accessed, acquired, or disclosed during such Breach; (d) steps that Individuals can take to protect themselves from potential harm from the Breach; and (e) a description of actions taken by Trend Micro to investigate the Breach, mitigate harm to individuals, and prevent further Breaches, see 45 CFR § 164.404(a)(2). Trend Micro’s obligation to report under this Section is not and will not be construed as an acknowledgement by Trend Micro of any fault or liability with respect to any Use, Disclosure, Security Incident, or Breach.

**2.4 Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2) of HIPAA, Trend Micro shall require its Subcontractors who create, receive, maintain, or transmit Protected Health Information on behalf of Trend Micro to agree in writing to: (a) the same or more stringent restrictions and conditions that apply to Trend Micro with respect to such Protected Health Information; and (b) comply with the applicable requirements of 45 CFR § 164 subpart C of the Security Rule. Trend Micro remains responsible for its Subcontractors’ compliance with the obligations of Trend Micro in this BAA.

**2.5 Mitigation.** Trend Micro agrees to mitigate, to the extent practicable, any harmful effect that is known to Trend Micro from a Use or Disclosure of PHI by Trend Micro inconsistent with its obligations under this BAA.

**2.6 Disclosure to the Secretary.** Trend Micro shall make available its internal practices, records, and books relating to the Use and/or Disclosure of Protected Health Information received from Company to the Secretary of the

Department of Health and Human Services for purposes of determining Company's compliance with HIPAA, subject to attorney-client and other applicable legal privileges.

**2.7 Accounting of Disclosure.** Trend Micro, at the request of Company, shall within fifteen (15) days make available to Company such information relating to Disclosures made by Trend Micro as required for Company to make any requested accounting of Disclosures in accordance with 45 CFR § 164.528 of the Privacy Rule.

**2.8 Designated Record Set.** The Parties agree that Trend Micro will not maintain PHI in a Designated Record Set for Company in connection with the Agreement and/or this BAA. If after the effective date of this BAA, Trend Micro shall specifically agree by amendment of the Agreement to maintain a Designated Record Set for Company, then and in that event, then Trend Micro, at the request of Company, shall provide access to Company of such Designated Record Set, and permit amendment of Protected Health Information therein contained in accordance with 45 CFR §§ 164.524 and 526.

**2.9 Performance of a Covered Entity's Obligations.** To the extent Trend Micro is to carry out a Covered Entity obligation under the Privacy Rule, Trend Micro shall comply with the requirements of the Privacy Rule that apply to Company in the performance of such obligation. Nothing in this BAA obligates Trend Micro to specifically carry out any Privacy Rule obligations. Company is required to specify in writing any future Privacy Rule obligations. Further, Trend Micro's products and services may not be subject to certain Privacy Rule obligations

### **3. COMPANY RESPONSIBILITIES WITH RESPECT TO PROTECTED HEALTH INFORMATION.**

**3.1 No Impermissible Requests.** Company shall not request Trend Micro to Use or Disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless otherwise permitted by HIPAA for a Business Associate).

**3.2 Contact Information for Notices.** Company hereby agrees that any reports, notification, or other notice by Trend Micro pursuant to this BAA may be made electronically. Company shall provide contact information to Trend Micro in such location or method as updated by Trend Micro from time-to-time and shall ensure that Company's contact information remains up-to-date during the term of this BAA. Contact information must include name of individual(s) to be contacted, title of individual(s) to be contacted, e-mail address of individual(s) to be contacted, name of Company organization, and, if available, Company's contract number(s). Failure to submit and maintain the aforementioned contact information may delay Trend Micro's ability to provide Breach notification under this BAA.

**3.3 Safeguards and Appropriate Use of Protected Health Information.** Company is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Company's obligation to:

- .1** Not include Protected Health Information in: (a) information Company submits to technical support personnel through a technical support request or to community support forums; and (b) Company's address book or directory information.
- .2** Implement privacy and security safeguards in the networks, systems, applications, and software Company controls, configures, and uploads in connection with Trend Micro Services.
- .3** Ensure that any Company employee/contractor communicating with Trend Micro about Company PHI or accessing Trend Micro systems that may contain such PHI have met all requirements specified by HIPAA (e.g., clearances and training).
- .4** Notify Trend Micro of any limitation(s) in the notice of privacy practices of Company under 45 § CFR 164.520, to the extent that such limitation may affect Trend Micro's Use or Disclosure of Protected Health Information.
- .5** Notify Trend Micro of any changes in, or revocation of, the permission by an individual to Use or Disclose his or her Protected Health Information, to the extent that such changes may affect Trend Micro's Use or Disclosure of Protected Health Information.
- .6** Notify Trend Micro of any restriction on the Use or Disclosure of Protected Health Information that Company has agreed to or is required to abide by under 45 § CFR 164.522, to the extent that such restriction may affect Trend Micro's Use or Disclosure of Protected Health Information.

### **4. PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION.**

**4.1 Trend Micro's Performance of its Obligations.** Except as otherwise limited in this BAA, Trend Micro may Use and Disclose PHI in order to perform functions, activities, and/or services agreed by the Parties and undertaken by Trend Micro as described in the Agreement, to the extent that such Use or Disclosure does not violate the Privacy Rule if done by Company. Trend Micro agrees to not Use or disclose PHI other than as permitted or required by this BAA or as Required by Law.

**4.2 Management, Administration, and Legal Responsibilities.** Except as otherwise limited in this BAA, Trend Micro may Use and Disclose Protected Health Information for the proper management and administration of Trend Micro and/or to carry out the legal responsibilities of Trend Micro, provided that any Disclosure may occur only if: (a) Required by Law; or (b) Trend Micro obtains written reasonable assurances from the person to whom the Protected Health Information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose for which it was Disclosed to the person, and the person notifies Trend Micro of any instances of which it becomes aware in which the confidentiality of the Protected Health Information has been breached.

**4.3 Reporting of Violations.** Trend Micro is authorized to Use and Disclose PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR §164.502(j)(1).

**4.4 Data Aggregation.** Except as may otherwise limited in this BAA, Trend Micro may use PHI to provide Data Aggregation services to Company as permitted by HIPAA.

## **5. TERM; TERMINATION.**

**5.1 Term.** This BAA shall continue in effect until the earlier of: (a) termination by a Party for breach as set forth in Section 5.2, or (b) expiration or termination of the Agreement.

**5.2 Termination for Breach.** When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Trend Micro shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer. Either Party may provide the other a ten (10) calendar day period to cure a material breach or default within such written notice.

### **5.3 Return, Destruction, or Retention of Protected Health Information Upon Termination.**

**.1** Upon expiration or termination of this BAA, Trend Micro shall return or destroy all Protected Health Information received from Company, created by Trend Micro, or otherwise in its possession, if it is feasible to do so, and as set forth in the applicable termination provisions of the Agreement or otherwise at the express written direction from the Company. This provision shall also apply to Protected Health Information that is in the possession of Subcontractors of Trend Micro.

**.2** If Trend Micro determines that it is not feasible to return or destroy any portions of the Protected Health Information upon termination of this BAA, Trend Micro shall inform Company of the conditions that make return or destruction infeasible. In that event, Trend Micro shall extend the protections of this BAA to such Protected Health Information (and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible) for so long as Trend Micro maintains such Protected Health Information.

**.3** Trend Micro and Company's respective rights and obligations under this Section 5.3 shall survive the termination of this BAA.

## **6. GENERAL PROVISIONS.**

**6.1 Interpretation.** The Parties intend that this BAA be interpreted consistently with their intent to comply with HIPAA and other applicable federal and state laws. Except where this BAA conflicts with the Agreement, all other terms and conditions of the Agreement remain unchanged. Any captions or headings in this BAA are for the convenience of the Parties and shall not affect the interpretation of this BAA.

**6.2 BAAs; Waiver.** This BAA may not be modified or amended except in a writing duly signed by authorized representatives of each of the Parties. A waiver with respect to one event shall not be construed as continuing, as a bar to, or as a waiver of any right or remedy as to subsequent events.

**6.3 No Third-Party Beneficiaries.** Nothing express or implied in this BAA is intended to confer, nor shall anything in this BAA confer, upon any person other than the Parties, and the respective successors or assigns of the Parties, any rights, remedies, obligations, or liabilities whatsoever.

**6.4 No Assignment Permitted.** This BAA may not be assigned, in whole or in part, without the express written consent of the Parties (which consent may be withheld discretion of each Party), and any attempted assignment in violation of this provision shall be void.

**6.5 Severability.** In the event that any provision of this BAA is found to be invalid or unenforceable, the remainder of this BAA shall not be affected thereby, but rather the remainder of this BAA shall be enforced to the greatest extent permitted by law.

**No Agency Relationship.** It is not intended that an agency relationship (as defined under the federal common law of agency) be established hereby expressly or by implication between Trend Micro and Company under HIPAA or the Privacy Rule, Security Rule, or Breach Notification Rule. No terms or conditions contained in this BAA shall be construed to make or render Trend Micro an agent of Company.