MASTER SERVICE AGREEMENT FOR BITDEFENDER BUSINESS SOLUTIONS AND SERVICES

THIS MASTER SERVICE AGREEMENT FOR BITDEFENDER BUSINESS SOLUTIONS AND SERVICES IS ENTERED BETWEEN THE VENDOR OF THE SERVICES, BITDEFENDER **("BITDEFENDER"),** AND CUSTOMER **("CUSTOMER").**

THE MASTER SERVICE AGREEMENT FOR BITDEFENDER BUSINESS SOLUTIONS AND SERVICES, TOGETHER WITH THE APPLICABLE SCHEDULES AND/OR STATEMENTS OF WORK AND THE PRIVACY POLICY AND ANY COMMERCIAL DOCUMENTATION PRESENTED TO CUSTOMER, SET FORTH THE TERMS AND CONDITIONS FOR THE PROVISION OF BITDEFENDER SOLUTIONS AND SERVICES, HEREINAFTER REFERENCED TOGETHER AS **"THE AGREEMENT**".

CUSTOMER REPRESENTS AND AGREES ON BEHALF OF ITS COMPANY THAT IT HAS THE CAPACITY AND AUTHORITY TO BIND THE COMPANY TO THIS AGREEMENT AND THAT IT HAS READ ALL THE TERMS AND CONDITIONS, UNDERSTAND THEM, AND AGREE TO BE BOUND BY THEM.

IF THE CUSTOMER IS AN MSP ACTING ON BEHALF OF THE CUSTOMER, CUSTOMER HAS THE OBLIGATION TO INFORM AND OBTAIN ITS CUSTOMERS' ACCEPTANCE ON THE TERMS OF THIS AGREEMENT.

IF THE CUSTOMER DOES NOT AGREE TO THIS AGREEMENT, THE CUSTOMER WILL NOT USE ANY BITDEFENDER SOLUTIONS AND SERVICES. BY CONTINUING OR BY USING OR BY INITIATING ANY BITDEFENDER SOLUTIONS AND SERVICES WITH BITDEFENDER IN ANY WAY, THE CUSTOMER IS INDICATING HIS COMPLETE UNDERSTANDING AND ACCEPTANCE OF THESE TERMS.

IF THE CUSTOMER DOES NOT AGREE TO ALL OF THESE TERMS, CUSTOMER MUST SEND AN EMAIL OF REFUSAL TO: LEGAL@BITDEFENDER.COM.

THIS AGREEMENT IS BINDING AS OF THE EARLIER OF: THE DATE CUSTOMER ACCEPTS IT OR THE DATE SET FORTH ON THE COMMERCIAL DOCUMENTATION.

An employee or other agent, including an MSP, reseller or contractor that installs or registers Bitdefender Solutions and Services on behalf of an entity, must be a representative of such entity and must accept this Agreement on behalf of the entity before Solutions and Services may be used. Please print this Agreement and save a copy electronically.

This Agreement is the entire legal agreement between Customer and Bitdefender for the initialization and use of the Services. This Agreement supersedes all agreements, understandings, and communications, whether written or oral between Customer and Bitdefender. Any of Customer's affiliates purchasing hereunder or using or accessing Services hereunder, or benefiting from the use of Solutions and Services, all listed herein, will be bound by, and comply with all terms and conditions of this Agreement. The entity accepting this Agreement will remain responsible for its Affiliates' acts and omissions unless otherwise agreed.

I. DEFINED TERMS

"Access Credentials" means any username and password or other security credentials that Customer or User must provide when accessing the Offensive Security Services or Cybersecurity Advisory Services via encrypted platform.

"**Affiliate**" means any entity in which Customer, as applicable, owns or controls, directly or indirectly, and any parent company that owns or controls, and any of the companies the parent company controls. For purposes of this definition, "control" means the direct or indirect beneficial

ownership of over fifty percent (50%) of the voting interests (representing the right to vote for the election of directors or other managing authority) in an entity.

"Authorized User"/" User" means a person that Customer authorizes to administer the use of the Offensive Security Services or of the Cybersecurity Advisory Services.

"**Agreement**" is the present Master Service Agreement for Bitdefender Business Solutions and Services as legal agreement between Bitdefender and Customer, for use of the Bitdefender Solutions and Services.

"**Beta Solution/ Early Access Solution/ Evaluation Solution/Trial**" means any trial or evaluation, or free solution of the Bitdefender Solutions and Services where available and any solution marked or otherwise designated as a beta, test version, early access or other evaluation form, irrespective of whether any payment has been made.

"Bitdefender IntelliZone Portal" is a cloud-based user interface solution, used to explore Threat Intelligence Data, SandBox Malware Analysis and Sandbox Malware Detection and may include associated media, printed materials, and any Documentation or any software updates and technical support.

"Bitdefender Threat Intelligence Solutions" means Operational Threat Intelligence Feeds, Reputation Threat Intelligence Feeds, Threat Intelligence API's, IntelliZone Portal, Sandbox Malware Analysis, and Sandbox Malware Detection further detailed and agreed in the Commercial Documentation such as agreements or purchase order as may be the case.

"Bitdefender Solutions" means collectively any Bitdefender software and the related services dedicated to companies identified in the Commercial Documentation and may include associated media, printed materials, and Documentation, and any software updates and technical support. To the extent permitted by applicable law, Bitdefender can modify its features, description and/or minimum system requirements, to continuously improve the quality and content of Bitdefender Solutions or Services.

"Commercial Documentation" any purchase order, quote or statement of work signed by the Customer and Bitdefender or its channel partners.

"Confidential Information" means non-public information in any form that is in the recipient's possession regardless of the method of acquisition that the discloser designates as confidential to recipient or should be reasonably known by the recipient to be confidential information due to the nature of the information disclosed and/or the circumstances surrounding the disclosure.

"**Customer**" refers to any legal entity as an end customer and MSP as a contractor of the end customer that has executed this Agreement and ordered Bitdefender Solutions and Services from Bitdefender or its authorized resellers or distributors, and as well Customer's Affiliates that places an order under this Agreement, uses or accesses any Bitdefender Solutions and Services for their internal use and not for redistribution.

"**Customer's Contractor**" means if the case, any services provider as individual or legal entity that has access or use of the Bitdefender Solutions and Services under this Agreement solely on Customer behalf and for Customer internal use, (ii) has an agreement to provide Customer the Bitdefender Solutions and Services, and (iii) is subject to confidentiality obligations and the terms of this Agreement.

"Customer Materials" means any items, documents, software, data, or other materials provided to Bitdefender by Customer during the performance by Bitdefender of the Offensive Security Services or Cybersecurity Advisory Services.

"Cybersecurity Advisory Services" means the following proactive consulting services provided by Bitdefender to support the management of cybersecurity risk which fall into three pillars: Strategy and Leadership, Risk and Compliance and/or Event Preparedness. The services are detailed in the SoW or on the Bitdefender websites, and may include associated media, printed materials, and Documentation.

"**Documentation**" means explanatory materials that may include written directions, policies, or associated media that accompany the Bitdefender Solutions and Services, which may be made available in printed, electronic, or online form on Bitdefender websites and which may be amended from time to time by Bitdefender.

“Internal Use” means the rights granted to the Customer under section 1.1. of Exhibit D.

“**MDR Services**” means the entire Bitdefender managed detection and response services portfolio as presented on Bitdefender websites or in other relevant service descriptions campaigning the Commercial Documentation and may include associated media, printed materials and Documentation, and any Updates and technical support as stated herein

“MDR Portal” means an online portal which provides access to MDR Services.

“MSP” means any services provider as legal entity that has access or use of the Bitdefender Solutions or Services under this Agreement solely on Customer’s behalf and for Customer’s internal use, (ii) has an agreement to provide Customer the Bitdefender Solutions and Services, and (iii) is subject to confidentiality obligations and the terms of this Agreement. Hereinafter, where the MSP is managing the Customer’s access to the Bitdefender Solutions and Services, all the references to Customer shall include MSP as well.

“Offensive Security Services” means the following services provided by Bitdefender: Bitdefender Offensive Security Services - Red Team Services and Bitdefender Offensive Services - Penetration Testing Services as detailed herein or in the SoW or on the Bitdefender websites, and may include associated media, printed materials, and Documentation.

“Offensive Security Services - Red Team Services” shall have the meaning of an intelligence-led assessment that simulates real-life threat actors to demonstrate how attackers would attempt to compromise the critical functions and underlying systems of Customer’s organization. It identifies security vulnerabilities (physical and/or digital) in the organization to help security team improve detection and response capabilities. Compared to a typical penetration test assessment, red teaming is goal-oriented and aims to assess the organization holistically by using Techniques, Tactics and Procedures (TTPs) driven by the MITRE ATT&CK Framework. More details are presented in the SoW agreed by parties or on the Bitdefender websites.

“Offensive Security Services - Penetration Testing Services” means the process of testing a target for exploitable security weaknesses in the Customer's security controls. Such weaknesses may be in areas such as authentication, authorization, validation and the targets of the penetration testing activity can include, without limitation: web applications, mobile applications, web Application Programming Interface (APIs), network devices, thick client applications, and wireless networks. Testing methodology may span from "black box testing"(where no knowledge is shared of the target) to "white box testing" (where maximum details of the target is shared, including where applicable source code, architecture diagrams, etc.). More details are presented in the SoW agreed by parties or on the Bitdefender websites.

“Operational Threat Intelligence Feeds” means Bitdefender TI APTs feed; Bitdefender TI Ransomware feed; Bitdefender TI Phishing and Fraud feed; Bitdefender TI C2 Servers feed; Bitdefender TI Mobile feed; Bitdefender TI Malicious IPs feed; Bitdefender TI Malicious Domains feed; Bitdefender TI Malicious URL feed; Bitdefender TI Malicious Files hashes feed.

“Professional Services” means any professional services performed by Bitdefender for Customer pursuant to a specific Commercial Documentation. Professional Services may include, without limitation: plan and design, offensive services, incident response, investigation and forensic services related to cyber-security adversaries, tabletop exercise and next generation penetration tests related to cyber-security or advisory services as they are presented on Bitdefender Websites or Commercial Documentation.

“Providing Services Use” means the rights granted to the Customer under section 1.2. of Exhibit D.

“Purchase Order” means the order signed by the Customer and Bitdefender for the Customer to access and use Bitdefender Threat Intelligence Solutions.

“Report” means the report and any documents, work products and related materials, provided by or on behalf of Bitdefender to Customer while performing the Offensive Security Services and/or Cybersecurity Advisory Services. For the avoidance of doubt, deliverables do not include fixes.

“Reputation Threat Intelligence Feeds” means Bitdefender TI IP-Reputation feed; Bitdefender TI Web Reputation feed; Bitdefender TI File Reputation feed; Bitdefender TI Vulnerabilities-extended feed.

“Sandbox Malware Analysis” is a cloud-based service which analyzes potentially harmful software in a Bitdefender controlled virtual environment, while observing the behavior of the malware and determining its intent. As a result, the service returns an analysis report for the submitted files or URLs.

“Sandbox Malware Detection” is a cloud-based service analyzing potentially harmful software in a Bitdefender cloud which will utilize various algorithms in order to recognize the files or URLs which are known to be malicious or clean and could have the potential to be malicious. If the file or URL could be classified by such algorithms alone as malicious or clean, a quick verdict will be returned without the file or URL being detonated. If a verdict will not be returned during this phase, the file or URL will be executed in a controlled virtual environment, while observing the behavior of the malware and determining its intent. As a result, Sandbox Malware Detection returns a verdict for the analyzed files and an analysis report for the malicious files.

“Services” mean collectively any service as the MDR Service, Professional Service, Offensive Security Services, Cybersecurity Advisory Services and the Cybersecurity Warranty Service and any other services offered to Customer by Bitdefender, its Affiliates or any of their vendors or providers and stated in the Commercial Documentation.

"Start Date" - means the day of purchase order or of placing the order within the Commercial Documentation (“Purchase Date’”), if the Bitdefender commercial partner is not selecting other date (“Standard Date”) or a later date selected in Commercial Documentation which cannot be later than 90 days from Purchase Date (“Preferred Date”).

“Statement of Work”, “SoW” means a document executed by both parties, where applicable, that details the Bitdefender Services purchased by Customer, including the description of the Bitdefender Services, the quantities, start and end dates, associated fees, if direct Customer towards Bitdefender, and other related details. If multiple SoWs are executed related to this Agreement, each SoW will be governed by this Agreement. SOWs are required to be executed for Professional Service, Offensive Security Services and Cybersecurity Advisory Services.

“Technical Data” means all electronic data stored on or transmitted by Customer to Bitdefender within the use of the Offensive Security Services and/or Cybersecurity Advisory Services such as any data or device information mainly, but not limited to data or device information related to threats, malicious websites and/or filenames, URLs, C&C Ips, hashes of various virus, malware threats which: (i) are collected from Customer by Bitdefender; (ii) are anonymized when knowing that such data may be deemed personal data, except for IPs, Mac addresses, computer names, command lines, filenames, URLs or the like (such that it is no longer personal data in accordance with applicable data protection law); (iii) cannot be linked to personal data; and (iv) are required by Bitdefender for the purposes of enhancing the security protection offered by Bitdefender solutions for the benefit of Customer and Bitdefender clients, and of improving and measuring the functionality or performance of Bitdefender technologies.

“Threat Intelligence API” means the functionality available from Bitdefender Cloud Service which Customer can query using Bitdefender Cloud Communication Protocol for a specific threat indicator and receive from the service a corresponding TI feed if such TI is available in the Bitdefender databases.

“Threat Intelligence Data” means the curated information on cyber threats in a machine-readable form including but not limited to information about malicious indicators such as URLs, Domains, IPs, files, Vulnerabilities, DarkWeb information, Control & Command servers, and Advanced Persistent Threats.

“**Update**” means an update to the detection data or software made available to Customer, or any correction, update, upgrade, patch, or other modification or addition at Bitdefender’s sole discretion, from time to time, but excluding any updates marketed and licensed for a separate fee.

"Upgrade" means any enhancement or improvement to the functionality of the Bitdefender Solutions made available to Customer at Bitdefender's sole discretion, from time to time, but excluding any new versions or software and/or upgrades marketed or provided for a separate fee.

"**User**" means Customer's employees, independent consultants or any other individual of Customer's organization who uses or has access to or benefits from Bitdefender Solutions and Services granted to Customer. For the purpose of "Providing Service Use", the Users shall mean the customers of the Customer using the Customer Service (see Exhibit D) as stated in the purchase order and for their internal use only.

"**Validity Period"** - means the timeframe when the Customer has the right to use Bitdefender Solutions or Services which shall begin on Start Date as stated in the Commercial Documentation, regardless of the number of copies that Customer is permitted to use and shall last for the period of time purchased as set forth in the Commercial Documentation, notwithstanding of its usage or not.

II. ORDERS AND PAYMENTS TERMS

1. Orders

1.1. Customer shall place orders for Bitdefender Solutions and Services to a Bitdefender partner (reseller or distributor) where the prices and payment terms shall be separately agreed between Customer and such Bitdefender partner. Alternatively, Customer may place orders directly to Bitdefender, if prior approved by Bitdefender. In such cases, the Parties shall conclude a separate order or SoW which shall contain the Bitdefender Solutions or Services, the quantities, subscriptions terms, prices and related payment details, and shall be governed by this Agreement.

1.2. All orders placed by Customer shall be governed by the terms and conditions of this Agreement and, if the order is place to a Bitdefender partner, also by the terms and conditions agreed with such Bitdefender partner.

1.3. Only those purchase orders/Commercial Documentation, with transaction-specific terms stating the Bitdefender Solutions and/or Services ordered, quantity, price, payment terms, term, and billing/provisioning contact information (and for the avoidance of any doubt, specifically excluding any pre-printed or standard terms of the Customer or Customer's contractors or MSPs) will have force or effect unless a particular Commercial Documentation is executed by an authorized signer of Bitdefender and returned to Customer or the applicable reseller. If any such Order or Commercial Documentation is so executed and delivered, then only those specific terms for that specific Order that expressly identify those portions of this Agreement that are to be superseded will prevail over any conflicting terms herein but only with respect to those Bitdefender Solutions and/or Services ordered on such Order.

1.4. The Orders or Commercial Documentation are non-cancellable. Any Order or Commercial Documentation through a reseller is subject to, and Bitdefender's obligations to Customer, are governed by this Agreement.

2. Payment and Taxes

2.1. The Customer will pay the fees for Bitdefender Solutions and/or Services directly or indirectly through Bitdefender channel partners as set forth in the applicable Order/SoW/Purchase Order/Commercial Documentation. Unless otherwise expressly set forth on the Order/SoW/Purchase Order/Commercial Documentation, Customer will pay the fees and amounts stated on each Order within 30 days from the invoice date. All invoices that are not paid within 30 days, and all credit accounts that are delinquent shall be assessed a 1% late payment charge (or if this exceeds the legally permitted maximum, the highest legal rate under applicable law) for each month the invoice is not paid, or the account is delinquent. Customer will reimburse Bitdefender or its resellers for all reasonable costs (including reasonable attorneys' fees) incurred by Bitdefender or its resellers in connection with collecting any overdue amounts.

2.2. Except as otherwise expressly provided in this Agreement, payment obligations are non-cancelable and fees and other amounts paid are non-refundable, and the purchased Bitdefender Solutions and Services cannot be decreased or exchanged for alternative services or subscriptions. Fees are exclusive of any applicable sales, use, value added, withholding, and other taxes, however designated. Customer shall pay all such taxes levied or imposed and the transactions hereunder, except for taxes based on Bitdefender's/its channel partners' income or with respect to Bitdefender's employment of its employees. All services and fees shall be consumed in the Validity Period agreed. No fees which are not consumed will survive the termination of the Validity Period.

3. Term

3.1. Term and duration of this Agreement shall start at the Activation Date of the Bitdefender Solutions and Services and shall follow the Validity Period of the respective Bitdefender Solutions and Services as specified in the Commercial Documentation related to the Order placed by Customer, in accordance with the Agreement.

3.2. For all Bitdefender Solutions and Services with yearly subscriptions, Customer will receive the activation codes or Services based on the solution acquired and Customer will have certain rights to use Bitdefender Solutions during the Validity Period, which shall begin on subscription Start Date as stated in the Commercial Documentation, regardless of the number of copies that Customer is permitted to use, and shall last for the Validity Period, when Bitdefender Solutions and Services will automatically be deactivated at the end of the Validity Period, and Customer will not be entitled to receive any feature or content updates to Bitdefender Solutions or Services.

3.3. For all Bitdefender Solutions and Services with monthly subscriptions, Customer will receive Bitdefender Solutions and services for as long as Customer pays for its subscription. If Customer fails to pay the monthly subscription, Customer's account will be suspended.

III. GENERAL LEGAL TERMS

1. INTELECTUAL PROPERTY RIGHTS

1.1. All rights not expressly set forth hereunder are reserved by Bitdefender.

1.2. Bitdefender Solutions and Services are protected by copyright and trade-secret laws and international treaty provisions. Therefore, Customer must treat Bitdefender like any other copyrighted material. Customer may not copy the printed materials accompanying Bitdefender Solutions and Services. Customer must produce and include all copyright notices in their original form for all copies created, irrespective of the media or form in which Bitdefender exists. Customer may not reverse engineer, de/recompile, disassemble, create derivative works, modify, translate, or make any attempt to reconstruct or to discover the source code for Bitdefender Solutions and Services or underlying ideas, algorithms, file formats, programming or functionality of Bitdefender Solutions and Services, unless otherwise allowed under the local legislation applicable to Customer.

1.3. All rights, titles and interest as well as all copyrights in and to Bitdefender Solutions and Services (including but not limited to know- how, images, photographs, logos, data, deliverables, animations, video, audio, music, text, "applets" incorporated into Bitdefender Solutions and Services), the accompanying printed materials are owned by Bitdefender or its licensors, with the understanding that rights, titles and interest in and to certain third-party software identified in the accompanying **Open-Source and Third-Party License Terms as published in the About sections** and they are owned by their respective owners. In respect of these Third-Party or open-source software, the following representations and liabilities clauses shall apply to the extent expressly required by the licenses, the terms of relevant licenses (including, in particular, the scope of license as well as disclaimers of warranties and liabilities) to the respective Third-Party software shall apply in lieu of this Agreement. Such **Third-Party License Terms** relating to respective software are located in the About section.

1.4. Customer may not remove any proprietary notices or labels on Bitdefender or its lawful owners. All rights not expressly set forth hereunder are reserved by Bitdefender or its lawful owners.

1.5. Customer acknowledges that the applicable Third-Party vendors are solely responsible for its offerings and Bitdefender makes no representations or warranties concerning those offerings and accepts no liability with respect to them, and if Customer uses any of these third-party offerings, the offerings and Customer's use of them will be governed by any license agreements, terms of use, privacy policies and/or other terms and conditions required by the third-party.

1.6. OPEN-SOURCE SOFTWARE IS PROVIDED BY BITDEFENDER "AS IS, WITH ALL FAULTS, AS AVAILABLE" WITHOUT (AND BITDEFENDER SPECIFICALLY DISCLAIMS) ANY GUARANTEE, CONDITION, OR WARRANTY (EXPRESSED, 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, BITDEFENDER 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 CUSTOMER OR BITDEFENDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. TECHNOLOGIES

2.1. Bitdefender informs Customer that in certain programs or products it may use data collection technology in order to collect technical information (including suspect files), solely to (i) improve the products, (ii) provide related services, (iii) adapt them to the latest industry trends and (iv) prevent the unlicensed or illegal use of the Bitdefender Solutions and Services or the damages resulting from any malware products identified. Customer hereby expressly agrees and accepts that Bitdefender may use such technical data collected / resulting information as part of the Bitdefender Solutions and Services provided in relation to the detection and to prevent and stop the malware programs running on Customer environment. Furthermore, Customer acknowledges and agrees that the security technology used can scan the traffic in an impersonal mode to detect the malware and to prevent the damages resulting from the malware products.

2.2. Customer acknowledges and accepts that Bitdefender may provide updates or additions to the services or products which automatically download to Customer's devices. Customer agrees that some of the executable files considered potentially harmful, may be submitted to Bitdefender servers for the purpose of such files being scanned.

2.3. Bitdefender reserves the right to collect certain information from the endpoints on which Customer has activated the Bitdefender Solutions or on which Services are performed, as the case may be, depending on the modules and features Customer has activated in Bitdefender Solutions and Services. Such information may pertain to potential security risks as well as to URLs of websites visited that Services or of Bitdefender Solutions deems potentially fraudulent. The URLs could contain personally identifiable information that a potentially fraudulent website is attempting to obtain without Customer's permission. As such, Customer agrees that certain modules, services and components may collect pieces of data from Customer systems for the purpose of evaluating and improving the ability of Bitdefender's products to detect malicious behavior, potentially fraudulent websites and other Internet security risks. Bitdefender also employs proprietary Cloud technologies to perform scanning on certain URLs, files or emails submitted from Customer systems. More details about the technical data collected are available on Bitdefender websites.

2.4. Bitdefender reserves the right to improve or change various features of its Bitdefender Solutions and Services or functionalities and features and to offer, from time to time, migration to the new available versions where such new versions shall also be governed by the same

terms and conditions presented in this Agreement. Customer expressly understands and accepts that these changes / modifications / migrations can be made unilaterally by Bitdefender, the only obligation of the latter being to notify the change (including by way of in-app or in-console notifications or emails or Bitdefender websites) in advance.

3. FEEDBACK

3.1. Customer may, from time to time, voluntarily elect to provide ideas, suggestions, comments, including without limitation ideas for new products, technologies, case studies, testimonials, promotions, product names, product feedback and product improvements ("Feedback") to Bitdefender with respect to Bitdefender Solutions and Services and Customer assigns to Bitdefender all rights, titles over Feedback, including allowing, without charge, royalties or other obligation to Customer, the right to make, have made, create derivative works, use, share and commercialize Customer's Feedback in any way and for any purpose. Customer will not give Feedback that is subject to a license that requires Bitdefender to license its software, technologies, or documentation to any third party because Bitdefender includes Customer's Feedback in them.

3.2. Customer expressly confirms that it has understood, acknowledged and agreed that if Customer provides such Feedback to Bitdefender that can't be assigned then, Customer shall grant Bitdefender the following worldwide, exclusive, perpetual, irrevocable, royalty free, fully paid up rights: (i) to make, use, copy, modify, sell, distribute, sub-license, and create derivative works of, the Feedback as part of any Bitdefender Solutions and Services , technology, service, specification or other documentation; (ii) to publicly perform or display, import, broadcast, transmit, distribute, license, offer to sell, and sell, rent, lease or lend copies of the Feedback (and derivative works thereof) as part of any Bitdefender Solutions and Services; (iii) to sublicense to third parties the foregoing rights, including the right to sublicense to further third parties; and (iv) to sublicense to third parties any claims of any patents owned or licensable by Customer that are necessarily infringed by a third party product, technology or service that uses, interfaces, interoperates or communicates with the Feedback or portion thereof incorporated into a Bitdefender Solutions and Services, technology or service. Further, Customer warrants that its Feedback is not subject to any license terms that would purport to require Bitdefender to comply with any additional obligations with respect to any Bitdefender Solutions and Services that incorporate any Feedback.

4. CONFIDENTIALITY

4.1. Neither Party shall disclose any confidential and/or proprietary information belonging to the other party unless agreed in writing by the said party and other than to its employees, and contractors, including without limitation, counsel, accountants, and financial advisors (collectively, "Representatives"), its Affiliates and their Representatives, subject to the other terms of this Agreement, and in each case who need to know such information and who are bound by restrictions regarding disclosure and use of such information comparable to and no less restrictive than those set forth herein. Confidential information shall not be limited to the terms and conditions of this Agreement, including its pricing provision, and all information clearly identified as confidential and includes any information regarding Bitdefender Solutions and Services.

4.2. This obligation shall not apply to information received which: (i) is or becomes known by the recipient without an obligation to maintain its confidentiality; (ii) is or becomes generally known to the public through no act or omission on the part of the recipient; or (iii) is independently developed by the recipient without the use of confidential or proprietary information; (iv) must be disclosed to any government authority or court of law as a result of a court order. If either Party is required to disclose confidential and proprietary information pursuant to law, recipient shall, to the extent legally permitted: (a) give discloser prompt written notice of such requirement or request prior to such disclosure; and (b) at discloser's cost, a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to recipient making such disclosure. If the recipient is legally required to disclose the discloser's Confidential Information

as part of: (a) a legal proceeding to which the discloser is a party but the recipient is not; or (b) a government or regulatory investigation of the discloser, the discloser shall pay all of the recipient's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) and will reimburse the recipient for its reasonable costs and fees of compiling and providing such Confidential Information, including, a reasonable hourly rate for time spent preparing for, and participating in, depositions and other testimony.

4.3. Each Party agrees to hold each other's confidential information in confidence for three years from the date of disclosure.

4.4. Customer acknowledges that a breach of this "Confidentiality" section shall cause Bitdefender irreparable injury and damages. Therefore, Customer agrees that such breach may be stopped through injunctive proceedings in addition to any other rights and remedies which may be available to Bitdefender at law or in equity.

4.5. Upon discloser's written request, recipient shall use commercially reasonable efforts to destroy the Confidential Information and any copies or extracts thereof. Upon discloser's request, recipient will provide Discloser with written confirmation of destruction in compliance with this provision. However, Recipient, its Affiliates and their Representatives may retain any Confidential Information that: (i) they are required to keep for compliance purposes under a document retention policy or as required by applicable law, professional standards, a court, or regulatory agency; or (ii) have been created electronically pursuant to automatic or ordinary course archiving, back-up, security, or disaster recovery systems or procedures; provided, however, that any such retained information shall remain subject to this Agreement.

5. EVALUATION/ BETA/TRIAL AND EARLY ACCESS LICENSES- applicable to the extent it is available for a particular Bitdefender Solutions or Services.

5.1. Where applicable and where Bitdefender offers Bitdefender Solutions or Services to Customer for evaluation, beta, trail or early access purposes ("Evaluation") the following terms and conditions shall apply in lieu of Section 2 - License Rights and Restrictions from Exhibit A, respectively Section 2 – Rights of Usage from Exhibit B : Bitdefender grants Customer a non-exclusive, temporary, royalty-free, non-assignable license to use Bitdefender Solutions or Service solely for internal non-production Evaluation. Such Evaluation license shall terminate (i) at the end date of the pre-determined Evaluation period, if an Evaluation period is pre-determined in Bitdefender Solution or Service or (ii) thirty (30) days from the date of Customer initial installation of Bitdefender Solution or Service, if no such evaluation period is pre-determined ("Evaluation Period"). Bitdefender Solution or Services may not be transferred and is provided "AS IS" without warranty of any kind. Customer is solely responsible for taking appropriate measures to back up its system and take other measures to prevent any loss of files or data. Bitdefender Solution may contain an automatic disabling mechanism that prevents its use after a certain period.

5.2. If Customer is an Evaluation user, Customer may use Bitdefender Solution for testing purposes in a non-production environment for a maximum of thirty (30) days from the date when Customer downloads Bitdefender Solution (the "Evaluation Period").

5.3. During any Evaluation Period, Customer can receive web or email based technical support in the country where Customer is located and Updates, only where it is available, without any guarantee or warranty of any kind.

5.4. THE PROVISIONS OF THIS SECTION WILL REPLACE SECTION "WARRANTIES" WITH RESPECT TO ANY EVALUATION SOLUTIONS.

TO THE FULLEST EXTENT PERMITTED BY THE APPLICABLE LAW, BITDEFENDER SOLUTION AND SERVICES USED FOR EVALUATION SOLUTIONS ARE PROVIDED TO CUSTOMER "AS IS", WITHOUT WARRANTIES OF ANY KIND.

BETA DISCLAIMER:

THE EVALUATION SOLUTION OFFERED HEREUNDER IS BELIEVED TO CONTAIN DEFECTS AND A PRIMARY PURPOSE OF THIS TESTING LICENSE IS TO OBTAIN FEEDBACK ON SOLUTION PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS

ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE SOLUTION AND/OR ACCOMPANYING MATERIALS.

WHERE LEGAL LIABILITY CANNOT BE EXCLUDED BY THIS DISCLAIMER, BUT MAY BE LIMITED, BITDEFENDER'S LIABILITY AND THAT OF ITS SUPPLIERS/LICENSORS/RESELLERS UNDER THIS AGREEMENT RELATED TO EVALUATION VERSION OF THE BITDEFENDER SOLUTION AND SERVICES, SHALL BE LIMITED IN THE AGGREGATE TO THE SUM OF TEN DOLLARS (USD$10.00) OR THE EQUIVALENT IN THE LOCAL CURRENCY.

5.5. FAIR USAGE. Bitdefender Solutions and Services shall have the following limitations unless otherwise agreed in the Commercial Documentation: a) the right to use it on up to three (3) Customer's Users concurrently, as defined in console; b) for maximum of (fifty) 50 endpoints per Customer and c) for a limited time period of maximum 2 (two) months from activation. In case of any violation of the limitations, Bitdefender reserves the right to terminate Customer rights at any time without any other further formalities.

5.6. Customer's right to use Bitdefender Solutions or Service ends when the Evaluation Period ends or if Customer violates any term of this Agreement or in case Customer will not respect or abuse in any way the licensing rights that were granted to Customer. Upon termination of the Evaluation Period, Customer must delete or destroy all copies of Bitdefender Solutions and Services and Documentation and stop using it.

6. WARRANTIES

6.1. Bitdefender warrants that Bitdefender Solutions and Services will be provided in a professional and workmanlike manner consistent with generally accepted industry standards.

6.2. Bitdefender warrants to Customer that the encoding of the software program on the media on which Bitdefender Solutions and Services are furnished will be free from defects in material and workmanship, and that Bitdefender Solution and Services shall substantially conform to its Documentation, for a period of ninety (90) days since Customer's Activation Date ("Warranty Period").

With respect to Bitdefender Solutions and Services, Customer must notify Bitdefender of any warranty claim during Warranty Period and within a maximum of 30 (thirty) days after the conclusion of the non-conforming Bitdefender Solutions and Services.

6.3. If Bitdefender is notified in writing of a breach of warranty during Warranty Period, Customer's sole and exclusive remedy and the entire liability of Bitdefender for its breach of this warranty will be for Bitdefender, at its option and expense, to use commercially reasonable efforts to: a) re-perform the non-conforming Bitdefender Solutions and Services or to correct, repair or replace Bitdefender Solution and Services within a reasonable time or (b) refund the portion of the fees paid attributable to the non-conforming Bitdefender Solutions and Services, after delivery of the proof of purchase.

Any replacement Solutions shall be warranted for the remainder of the original Warranty Period.

6.4. In addition to the other exclusions stated in the Agreement, also Warranty shall not apply if (i) the Bitdefender Solutions and Services have not been used in accordance with the terms and conditions of this Agreement and the Documentation; (ii) the issue has been caused by Customer's failure to apply Updates or any other action or instruction recommended by Bitdefender, (iii) the issue results from any cause outside of Bitdefender's reasonable control, (iv) in the event of failure of Bitdefender Solutions and Services 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; (iv) if any problem or error in Bitdefender Solutions and Services have resulted from improper use, misapplication or misconfiguration, or the use of Bitdefender Solution and Services with other programs or services that have similar functions or features which are incompatible with Bitdefender Solution and Services; (v) if Bitdefender Solution and Services offered or used as any

Evaluation version or for add-ons or free Bitdefender Solutions or Services for which Bitdefender does not charge; or (vi) if Bitdefender does not receive notice of a non-conformity within the applicable Warranty period.

6.5. BITDEFENDER SOLUTIONS AND SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT BITDEFENDER DOES NOT GUARANTEE THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER' SYSTEM THREATS, VULNERABILITIES, INCIDENTS, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER WILL NOT HOLD BITDEFENDER RESPONSIBLE THEREFORE BITDEFENDER DOES NOT WARRANT THAT BITDEFENDER SOLUTIONS AND SERVICES WILL MEET CUSTOMER'S REQUIREMENTS. BITDEFENDER DOES NOT GUARANTEE THAT THE BITDEFENDER SOLUTIONS AND SERVICES WILL PERFORM ERROR-FREE OR UNINTERRUPTED OR THAT BITDEFENDER WILL CORRECT ALL PROGRAM ERRORS OR THAT THE CUSTOMER'S SYSTEMS WILL BE SECURE, ERROR-FREE, UNINTERRUPTED OR COMPLIANT.

6.6. TO THE EXTENT PERMITTED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, BITDEFENDER HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED OR EXPRESS WARRANTIES AND CONDITIONS, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES, WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO ANY RECOMMENDATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, LOSS OF DATA, FALSE POSITIVES OR FALSE NEGATIVES, DEVICE FAILURE OR MALFUNCTION TITLE, NON-INTERFERENCE, TIMELINESS, COMPLETENESS, CURRENTNESS, RELIABILITY ACCURACY OF INFORMATIONAL CONTENT, SYSTEM INTEGRATION, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS BY FILTERING, DISABLING, OR REMOVING SUCH THIRD PARTY'S SOFTWARE, SPYWARE, ADWARE, COOKIES, EMAILS, DOCUMENTS, ADVERTISEMENTS OR THE LIKE, NOR THAT BITDEFENDER SOLUTIONS AND SERVICES WILL DETECT ANY OR ALL SECURITY INCIDENTS, SECURITY OR MALICIOUS CODE THREATS OR USE OF BITDEFENDER SOLUTIONS AND SERVICES AND OTHER SERVICE, FUNCTIONALITIES, FEATURES, ENHANCEMENTS, MAINTENANCE OR SUPPORT RELATED THERETO, OR ANY OTHER MATERIALS (TANGIBLE OR INTANGIBLE) AND ANY UPDATES SUPPLIED BY BITDEFENDER WILL KEEP CUSTOMER'S NETWORK, CLOUD OR ENDPOINTS OR ANY SYSTEMS AND DEVICES FREE FROM MALWARE OR OTHER MALICIOUS OR UNWANTED CONTENT, OR UNINTERUPTED OR SAFE FROM INTRUSIONS OR OTHER SECURITY ATTACKS/SCAMS/BREACHES.

6.7. CUSTOMER UNDERSTANDS AND AGREES THAT BITDEFENDER CANNOT, AND DOES NOT HEREIN, PROVIDE ANY WARRANTY, GUARANTEE, CONDITION, OR ASSURANCE THAT THE DEPLOYMENT/USE OF ANY BITDEFENDER SOLUTIONS AND SERVICES(EITHER BY ITSELF OR IN COMBINATION WITH OTHER BITDEFENDER SOLUTION AND SERVICES) WILL BE ERROR FREE, UNINTERUPTED, NOR WILL GUARANTEE COMPLETE PROTECTION FROM AND AGAINST ALL PRESENT AND FUTURE SECURITY THREATS TO CUSTOMER'S NETWORKS, SYSTEMS, DEVICES, SERVERS OR DATA AND NOTHING HEREIN SHALL BE DEEMED TO IMPLY SUCH A WARRANTY, GUARANTEE, CONDITION, OR ASSURANCE. FURTHERMORE, BITDEFENDER DOES NOT PROVIDE ANY WARRANTY, GUARANTEE, CONDITION, OR ASSURANCE OR LEGAL ADVICE IN REGARD OF DIFFERENT LAWS, REGULATIONS, CERTIFICATIONS, POLICIES OR STANDARDS IMPLEMENTATION.

6.8. BITDEFENDER SOLUTIONS AND SERVICES ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. BITDEFENDER SOLUTIONS AND SERVICES ARE NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPON SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY/ENVIRONMENTAL DAMAGES.

6.9. Due to the continual development of new techniques for attacking endpoints, networks, systems, Bitdefender does not represent, warrant or guarantee: (1) that Bitdefender Solutions and Services will detect, block, or completely remove, or clean any or all applications, routines, and files that are malicious, fraudulent or unwanted; or (2) that any product or any data, equipment, system or network on which a Bitdefender Solutions and Services are used (or protects) will be free of vulnerability to intrusion or attack.

6.10. Customer agrees that protection of its endpoints, servers, cloud, networks, servers and data are dependent on factors solely under Customer'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 assure business continuity and 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 or PPAs; (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 made available by Bitdefender.

6.11. CUSTOMER SHALL BE SOLELY RESPONSIBLE FOR THE PROPER BACK-UP OF ALL DATA AND CUSTOMER SHALL TAKE APPROPRIATE MEASURES TO PROTECT SUCH DATA AND ASSURE BUSINESS CONTINUITY. BITDEFENDER ASSUMES NO LIABILITY OR RESPONSIBILITY WHATSOEVER IF DATA IS LOST OR CORRUPTED OR SYSTEM INTERUPTIONS.

7. INDEMNITIES

7.1. Customer and MSP shall indemnify, defend, and hold Bitdefender and its directors, officers, employees, agents and attorneys harmless from and against any and all third-party claims, actions, demands, liabilities, losses, damages, judgments, or settlements, including all reasonable attorney's fees, and expenses related thereto, directly or indirectly resulting from, relating to, arising out of, or attributable to or based upon, Customer's miss-use of Bitdefender Solution and Services or in violation of any third party rights.

7.2. Bitdefender shall defend, indemnify and keep Customer harmless from any claim by a third party, that Customer' use of Bitdefender Solutions and Services by Customer, in accordance with the terms and conditions of this Agreement, infringes that third party's intellectual property rights, and against the resulting costs and damages finally awarded against Customer to such third party by a court of competent jurisdiction or agreed in a settlement.

7.3. The foregoing obligation of Bitdefender does not apply with respect to software, services or portions or components thereof: (i) not supplied by Bitdefender; (ii) used in a manner not expressly authorized by this Agreement or the accompanying Documentation (iii) made in accordance with Customer's specifications; (iv) modified by anyone other than Bitdefender, if the alleged infringement relates to such modification; (v) combined with other products, processes or materials where the alleged infringement would not exist but for such combination; (vi) any third party software or services or open source software or and Evaluation Solution or Services or offer for no cost to Customer or where Bitdefender does not charge for it or (vii) where Customer continues the allegedly infringing activity after being notified thereof and provided with modifications that would have avoided the alleged infringement.

7.4. In the event the Bitdefender Solutions and Services are held by a court of competent jurisdiction to constitute an infringement of third party intellectual property rights, Bitdefender shall, at its sole option, do one of the following: (i) procure the right to continued use; (ii) modify Bitdefender Solutions and Services, as the case may be, so that their use becomes non-infringing; (iii) replace Bitdefender Solutions and Services, as the case may be, with substantially similar products in functionality and performance; or (iv) if none of the foregoing alternatives is reasonably available to Bitdefender, Bitdefender shall refund the pro-rata unused portion of Bitdefender Solutions or Services, depending on the case.

7.5. The Parties may request indemnification under this provision, provided they: (a) give notice within ten (10) days of any claim being made or proceedings being issued against; (b) give sole control of the defense and settlement to the indemnifying party (provided any settlement relieves

the indemnified party of all liability in the matter); (c) provide all available information and reasonable assistance; and (d) have not previously compromised or settled such claim without the other party prior approval.

THIS SECTION STATES BITDEFENDER'S ENTIRE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR INFRINGEMENT AND MISAPPROPRIATION CLAIMS.

8. LIABILITY. LIMITATION OF LIABILITY

8.1. BITDEFENDER SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR ANY LOSS OF PROFITS, REVENUE, DATA, OR DATA USE OR DAMAGES THAT WERE REASONABLY FORESEEABLE BY BOTH PARTIES BUT COULD HAVE BEEN PREVENTED SUCH AS, FOR EXAMPLE, LOSSES CAUSED BY VIRUSES, MALWARE, ERRORS, SYSTEM INTERRUPTIONS OR OTHER MALICIOUS PROGRAMS, OR LOSS OF OR DAMAGE TO CUSTOMER DATA OR SYSTEM INTERRUPTIONS.

8.2. THE TOTAL BITDEFENDER's MAXIMUM LIABILITIES OR INDEMITIES FOR ANY DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER ARISING BY STATUTE, LAW, COURSE OF DEALING, CUSTOM AND PRACTICE, OR TRADE USAGE SHALL BE LIMITED AND IN NO CASE SHALL BITDEFENDER'S LIABILITY EXCEED THE FEES CUSTOMER PAID TO BITDEFENDER FOR THAT DEFICIENT BITDEFENDER SOLUTIONS OR SERVICES IN THE LAST 12 MONTHS IMMEDIATELY PRECEDING THE EVENT OR CIRCUMSTANCE FIRST GIVING RISE TO A CLAIM UNDER THIS AGREEMENT.

SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO CUSTOMER.

8.3. NOTWITHSTANDING THE FOREGOING, BITDEFENDER DOES NOT LIMIT OR EXCLUDE ITS LIABILITY FOR (i) DEATH OR PERSONAL INJURY CAUSED BY GROSS NEGLIGENCE DIRECTLY ATTRIBUTABLE TO BITDEFENDER, (ii) FRAUDULENT MISREPRESENTATION, OR (iii) ANY OTHER LIABILITY TO THE EXTENT THAT SUCH LIABILITY CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

8.4. 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 absence of any 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.

8.5. Bitdefender is acting on behalf of its partners for the purpose of disclaiming, excluding and/or limiting obligations, warranties and liability as provided in this Agreement. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

9. PRIVACY POLICY & GDPR

9.1. All the information on how the personal data is processed during the usage of the Bitdefender Solutions and Services is specified in the Bitdefender Privacy Policy published on: https://www.bitdefender.com/site/view/legal-privacy-policy-for-bitdefender-business-solutions.html as well as about the Personal Data Notice for Business Contacts of the Clients/Partners published on: https://www.bitdefender.com/site/view/legal-personal-data-notice-for-business-contacts-of-the-clients-or-partners.html.

With respect to personal data collected by Bitdefender Solutions and Services from Customers' Users and the applicable data protection legislation governing this relationship, according to the EU applicable legislation on personal data (GDPR – General Data Protection Legislation), Bitdefender together with Customer are joint controllers. Bitdefender acts as a data controller in relation to the personal data collected through its products and services sold to/through business clients only for the purposes of ensuring cyber security, including support activities for this purpose (only in specific cases, when support activities are included in the specific contract with Bitdefender). The Users also act as data controllers in relation to the personal data they might have access to through Bitdefender Solutions and Services for purposes of ensuring information and network security. For any other potential purposes that business Users may decide upon internally on their own, business clients and service providers (and their clients) act as separate and independent data controllers, collecting personal data from another source, meaning Bitdefender`s solutions and services.

The joint controllers will be each independently and separately responsible for respecting the GDPR provisions, including lawful processing of personal data, informing service users on the use of their personal data, the security of such personal data and making sure Service users can exercise their rights, according to the Joint Controllers Arrangement available here: https://www.bitdefender.com/media/materials/legal/Joint-Controllers-Arrangement.pdf.

9.2. Notwithstanding the previous provisions in this chapter, with regard to data processed by certain Bitdefender Solutions and Services as enumerated below in article 9.3, Bitdefender acts as a data processor in relation with the personal data collected through these Bitdefender Solutions and Services for the purposes of Customer internal security management.
In this case, Customer acts as data controller in relation to the collected personal data by customizing the securities rules, policies, solution settings and/or the duration of data storage as applicable when using Bitdefender Solutions and Services.

9.3 The following Bitdefender Solutions and Services where Bitdefender acts as Data Processor are: Bitdefender Integrity Monitoring, Bitdefender GravityZone Security for Mobile Solution, Bitdefender Cloud Security, Bitdefender Offensive Security Security and Cybersecurity Advisory Services. Customer is strictly responsible for complying with the GDPR provisions, including lawful processing of personal data, informing Customer users about the use of their personal data, the security of personal data and ensuring Customer's users can exercise their rights, according to the Data Protection Agreement available here: https://www.bitdefender.com/site/view/data-processing-agreement-for-bitdefender-solutions.html.

10. TECHNICAL SUPPORT. SERVICES

10.1. Technical support for Bitdefender Solutions and Services is included for the Validity Period. Certain technical support features may be offered by Bitdefender through its resellers for the Validity Period of Bitdefender Solutions and Services as stated on Bitdefender website. Technical Support shall be governed by the following conditions: Any such Technical Support shall be provided without any guarantee or warranty of any kind. It is solely the Customer's responsibility to complete a backup of all its existing data, software, and programs before receiving any Technical Support.

Standard Technical Support. The terms and conditions of standard technical support for Bitdefender GravityZone Enterprise are stated here: http://www.bitdefender.com/site/view/enterprise-support-policies.html.

10.2. Paid Services:

10.2.1. Professional Services: If Customer purchases these Services, their performance will be according to the Service Level Agreement available at the following address:

https://www.bitdefender.com/media/materials/legal/Service-Level-Agreement-for-Professional-Services.v1.1.pdf.

Professional Services hours prepaid under a retainer must be used within one year from the date of the SoW or Order. Additional blocks of hours purchased under the retainer will expire one year from the effective date of the corresponding Order or SoW for additional hours.

10.2.2. Premium Technical Support Services: If Customer purchases these services, their performance will be according to the Enterprise Support Policy available at: https://www.bitdefender.com/site/view/enterprise-support-policies.html.

10.2.3. Offensive Security Services and Cybersecurity Advisory Services: If Customer purchases these Services, their performance will be according to this Agreement including the Special Terms and Conditions from Exhibit C herein attached.

10.2.4. MDR Service: If Customer purchases these Services, their performance will be according to this Agreement including the Special Terms and Conditions from Exhibit B herein attached.

10.3. Bitdefender reserves the right to refuse, suspend or terminate any of the Technical Support, either Standard or Premium per the above, in its sole discretion in case the Customer is in breach of its obligations. The Technical Support policies are subject to change at Bitdefender's discretion; however, Bitdefender will not materially reduce the level of services provided for supported programs during the period for which fees for Technical Support have been paid.

10.4. Customer should review the policies published on websites prior to entering the ordering document for the applicable Services. If Customer intends to receive any Professional Services, then Customer needs to sign a separate statement of work with Bitdefender. These terms are not applicable for Trial and Beta Solutions.

11. SYSTEM REQUIREMENTS. CUSTOMER'S OBLIGATONS.

11.1. Customer and MSP are responsible for middleware, miscellaneous software, and software applications installation. This responsibility covers correct licensing, configurations control, administration, and operations readiness. Customer and MSP are responsible for the installation, operation, maintenance, and support of any software that is not expressly under the sole responsibility of Bitdefender. The customer and MSP agree to inform Bitdefender via email about the progress of the site preparation, delivery, installation, configuration, and completion of the tests of the configuration.

11.2. Customer acknowledges that technologies are not universally compatible and that there may be limitations. Customer and MSP understand and agree that Customer and MSP have the sole responsibility for maintaining and backing up data. In all cases, the Customer and MSP agree to hold Bitdefender harmless from any losses resulting from the loss of data during performance of Bitdefender Solutions and Services or otherwise. In addition, Customer and MSP are solely responsible for the protection of passwords and Bitdefender shall in no way be responsible for any password loss, password change or password incompatibility, even if such password was initially generated by Bitdefender or any third-party software. Please be advised that in such a scenario (i.e. a generated password), Bitdefender strongly advises the Customer to change such automatically generated password after first introducing it along with any other credentials into any piece of software.

11.3. Obligations**.** Customer, along with MSP and Affiliates, represents and warrants that: (i) own or have a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Bitdefender Solutions and Services will be installed or that will be the subject of, or investigated during Validity Period of the Bitdefender Solutions and Services (ii) to the extent required under any federal, state, or local U.S. or non-US laws Customer authorized Bitdefender to access these Systems and process and transmit data through in accordance with this Agreement and as necessary to provide and perform the Bitdefender Solutions and Services, (iii) have a lawful basis in having Bitdefender investigate the Systems, process the Users' Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct Bitdefender to provide the Bitdefender Solutions and Services, and (v) Customer has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Users Data and Personal Data from each User or Affiliate, to Bitdefender.

11.4. Customer agrees to use Services in accordance with laws, rules and regulations and acknowledges that Customer is solely responsible for determining whether a particular use of Bitdefender Solutions and Services is compliant with such laws. Customer must obtain all necessary rights and permissions from its Users to use Bitdefender Solutions and Services. Customer is liable and responsible for all actions and omissions occurring under its Users' accounts.

12. SPECIAL TERMS FOR MSP

12.1. Customer authorizes Bitdefender to give MSP the rights and privileges to Bitdefender Solutions and Services necessary to enable and provide for use and receipt of its services to Customer. If at any time Customer revokes this authorization, then Customer will be responsible for taking all actions necessary to revoke such access and use in Bitdefender Solutions and Services and Customer will disable its access to Bitdefender Solutions and Services within a reasonable period of time. If Customer would need Bitdefender assistance, please contact Bitdefender support.

12.2. Disclaimer.

Customer as well as MSP remain responsible for their acts and omissions during such time. Bitdefender Solutions and Services are not conditional upon MSP's usage. Bitdefender is not responsible or liable for any loss, costs or damages arising out of their actions or inactions in any manner, including but not limited to, for any disclosure, transfer, modification, or deletion of data. Bitdefender: (i) does not control, monitor, maintain or provide support to MSP, (ii) disclaims all warranties of any kind, indemnities, obligations, and other liabilities in connection with MSP services provided to Customer, and any of MSP' interface or integration with the Services. Customer hereby acknowledges and agrees that Bitdefender cannot be held liable for any services and related features provided by MSP, which might no longer be available to Customer for any reason.

Customer should not give or allow MSP access to, or use of, intelligence reports provided by, or made accessible in the Bitdefender Solutions or Services.

13. ELECTRONIC COMMUNICATIONS

13.1. Bitdefender may send Customer legal notices and other commercial communication about the Bitdefender Solutions and Services (including updates, new features or services) or use the information that Customer provides Bitdefender ("Communications"). Bitdefender will send Communications via in-product notices or via email to the primary user's registered email address or will post Communications on its Sites. The legal basis for sending these communications is this Agreement (for the Commercial communications) and the legitimate interest for marketing with the current customers for the commercial Communications. With respect to email notices, any such email notice to Customer will be sent by Bitdefender to the account administrator(s) or other contacts named by Customer during registration. Customer is responsible for ensuring that the email address for the account administrator or contact info is accurate. Any email notice that Bitdefender sends to the then-current email address will be effective when sent, whether or not Customer actually receives the email.

14. EXPORT

14.1. Each party agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to such party in the performance of this Agreement, including but not limited to, applicable export and import, anti-corruption and employment laws. Customer acknowledges and agrees the Bitdefender Solutions and Services shall not be used, transferred, or otherwise exported or re-exported to regions that the United States and/or the European Union maintains an embargo or comprehensive sanctions (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions under any applicable laws (e.g., parties listed on the U.S.

Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "Designated Nationals"), without first obtaining all required authorizations from the U.S. government and any other applicable government. Customer and MSP represent and warrant that Customer, Customer's Contractors or Affiliates are not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National. Also, Bitdefender represents and warrants that is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National. Customer and MSP agree to indemnify and hold Bitdefender harmless from and against claims, losses, costs, or liability, arising in connection with breach of these obligations by Customer.

15. SUSPENSION AND TERMINATION

15.1. This Agreement shall remain effective for Validity Period of the Bitdefender Solutions and Services according to the Commercial documentation or until termination in accordance with this section or as otherwise specified herein. Bitdefender may immediately suspend Customer access to, or use of, the Bitdefender Solutions and Services if: (i) Bitdefender believes that there is a significant threat to the security, integrity, functionality, or availability of the Services or Bitdefender Solutions or any content, data, or applications in thereof; (ii) Customer or Customer's Users are in breach of rights granted under the Agreement; or (iii) failure of payment to Bitdefender; provided, however, Bitdefender will use commercially reasonable efforts under the circumstances to provide Customer with notice and, if applicable, an opportunity to remedy such violation prior to any such suspension.

15.2. In case of Services, either party may terminate this Agreement upon 30 (thirty) days' written notice for an uncured material breach, not remedied in the 30 (thirty) days' notice period.

15.3. Further, if Customer does not comply with the terms of this Agreement, Customer acknowledges that it has no right to use Bitdefender Solutions and Customer agrees to uninstall or not use Bitdefender Solutions and Services.

15.4. For the avoidance of doubt, for Evaluation Solutions, after the termination of the Evaluation period, Bitdefender shall have no further obligation to Customer.

15.5. Bitdefender reserves the right to revoke Customer right to use Bitdefender Solutions and Services if the Customer does not comply the terms of this Agreement. In case of termination of this Agreement due to material breach of Customer's obligations, Bitdefender shall have no obligation to provide notice and will stop Customers' access to Bitdefender Solutions or Services immediately.

15.6. Bitdefender reserves the right to stop supporting its products or a version of its products or discontinue its Solutions or Services or product features. End-of-support policies are posted on Bitdefender website and may be consulted at the following link: https://www.bitdefender.com/support/bitdefender-end-of-life-policy-statement-982.html.

16. AUDIT RIGHTS

16.1. Bitdefender may audit Customer's use of Bitdefender Solutions and Services to verify that Customer usage complies with applicable Documentation. An audit will be done upon reasonable notice and during normal business hours, but not more often than once each year unless a material discrepancy was identified during the course of a prior review. Customer agrees to implement internal safeguards to prevent any unauthorized copying, distribution, installation, or use of, or access to Bitdefender Solutions and Services. Customer further agrees to keep records sufficient to certify Customer compliance with this Agreement, and, upon request of Bitdefender, provide and certify metrics and/or reports based upon such records and accounting for both numbers of copies (by Solution and version) and network architectures as they may reasonably relate to Customer subscription and deployment of Bitdefender Solutions and Services.

16.2. If an audit reveals any deployment or use of Bitdefender Solution and Services that is more than the subscriptions conditions or is otherwise out of compliance with this Agreement, then Customer agrees to promptly correct such non-compliance. If the usages for any

unlicensed or excess utilization of all solutions audited hereunder is greater than, in the aggregate, five percent (5%) of the actual licensed use for solutions purchased by Customer, Customer agrees to reimburse Bitdefender for the differences and its reasonable costs incurred in performing the audit.

17. FORCE MAJEURE

17.1. Neither Party shall be in breach of the Agreement in the event it is unable to perform its obligations because of a natural disaster, war, emergency conditions, strikes, acts of terrorism, the substantial inoperability of the Internet, the inability to obtain supplies, or any other reason or condition beyond its reasonable control. If such reasons or conditions remain in effect for a period of more than thirty (30) calendar days, either Party may terminate the Agreement affected by such force majeure following the written notice to the other Party. Notwithstanding the aforementioned, the Parties agree that payment obligations derived from this Agreement shall not be delayed for any reason.

18. MISCELANEOUS

18.1. If Customer is located in the United States or Canada, this Agreement is governed by the laws of the State of Florida, USA, with the venue in Broward County. If Customer is located in the UK, Australia and New Zeeland, this Agreement will be governed by the laws of UK laws, with the venue in Reading. If Customer is located in the Netherlands, Belgium, Denmark, Finland, Iceland, Norway, and Sweden, this Agreement is governed by the Dutch Laws with the venue in the Hague. If Customer is located in Germany and Austria, this Agreement is governed by the German Laws with the venue in München. If Customer is located in Indonesia or in Singapore, this Agreement will be governed by the laws of Singapore with the venue in the courts of Singapore. If Customer is located in rest of Europe, in the rest of Asia, Africa and Middle East, LATAM, this Agreement will be governed by the laws of Romania with the venue in the courts of Bucharest.

18.2. In the event of invalidity of any provision of this Agreement, the invalidity shall not affect the validity of the remaining portions of this Agreement.

18.3. This Agreement describes certain legal rights. Customer may have other rights under the laws of Customer state or country. Customer may also have rights with respect to the party from whom Customer acquired Bitdefender Solutions and Services. This Agreement does not change Customer rights or obligations under the laws of Customer state or country if the laws of Customer state or country do not permit it to do so.

18.4. Bitdefender and Bitdefender logos are trademarks of Bitdefender. All other trademarks used in Bitdefender Solutions and Services or in associated materials are the property of their respective owners.

18.5. Bitdefender retains the right to assign this Agreement in its sole discretion. Customer may not assign this Agreement without the prior written permission of Bitdefender, provided, however, that Customer shall have the right to transfer this Agreement by operation of law as part of a merger, reorganization, or sale of all or substantially all of Customer assets or shares upon written notice to Bitdefender.

18.6. Either party represents and warrants that (i) in connection with this Agreement, it has not and will not make any payments or gifts or any offers or promises of payments or gifts of any kind, directly or indirectly, to any official of any foreign government or any agency or instrumentality thereof and (ii) it will comply in all respects with the Foreign Corrupt Practices Act and any other applicable laws and (iii) it will comply with the export compliance laws applicable to each party fulfilling its obligation under this Agreement. 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 enacted hereafter (such as Contracts (Rights of Third Parties) Act of 1999 in the UK and similar laws enacted in Ireland, Singapore, New Zealand, 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 expressed 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, Bitdefender's suppliers, software licensors, and resellers shall be intended third party beneficiaries for the exclusions, limitations, and disclaimers with respect to Bitdefender Solutions and Services as stated in this Agreement.

18.7. This Agreement constitutes the entire agreement between Customer and Bitdefender concerning the subject matter of this Agreement and it supersedes all prior and simultaneous proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. It is expressly agreed that the terms of this Agreement shall supersede any terms in any procurement Internet portal or other similar non- Bitdefender document and no such terms included in any such portal or other non- Bitdefender document shall apply to the Bitdefender Solutions and Services ordered. Any Order or other Commercial Documentation through a reseller is subject to, and Bitdefender's obligations and liabilities to Customer are governed by, this Agreement. Bitdefender is not obligated under any agreement or order made by the Reseller with Customer unless a legal representative of Bitdefender executes the agreement.

18.8. Bitdefender may revise these terms and conditions of the Agreement at any time and the revised terms shall automatically apply to the corresponding versions of Bitdefender Solutions and Services distributed with the revised Agreement. If any part of this Agreement is found void and unenforceable, it will not affect the validity of the rest of the Agreement, which shall remain valid and enforceable. In case of controversy or inconsistency between translations of this Agreement to other languages, the English version issued by Bitdefender shall prevail.

Any additional, conflicting, or different terms or conditions proposed by Customer or Customer contractors or MPSs or any of Customer issued documents, Commercial Documentation, are hereby rejected by Bitdefender and excluded here from.

18.9. This Agreement shall govern the relationship between the parties with respect to all Commercial Documentation for the Bitdefender Business Solutions and Services that Customer shall place either directly to Bitdefender or through a Bitdefender partner.

18.10. Unless Customer informs Bitdefender otherwise by sending an email to us at legal@bitdefender.com, at any time, Customer agrees that Bitdefender may display Customer's company name and logo (in accordance with any trademark guidelines Customer provides) as a Bitdefender customer in a manner that does not suggest Customer's use or endorsement of any specific Bitdefender Solutions and Services not provided to Bitdefender.

18.11. For matters related to support the following terms shall apply: https://www.bitdefender.com/business/customer-portal/enterprise-standard- support.html. For legal notices, Customer the contact address is: legal@bitdefender.com.

The present Agreement is comprised of its provisions together with the following:

Exhibit A – "Specific Terms and Conditions for Bitdefender Solutions"

Exhibit B – "Specific Terms and Conditions for MDR Services and Cybersecurity Warranty Service"

Exhibit C – "Specific Terms and Conditions for Offensive Security Services and Cybersecurity Advisory Services

Exhibit D – "Specific Terms and Conditions for Threat Intelligence Services"

where all together are collectively referred to this MASTER SERVICE AGREEMENT FOR BITDEFENDER BUSINESS SOLUTIONS AND SERVICES.

Exhibit A - SPECIAL TERMS AND CONDITIONS FOR BITDEFENDER SOLUTIONS

1. SOLUTION REGISTRATION.

1.1. Registration of a Bitdefender Solution requires a valid Bitdefender Account that includes a valid email address for receiving Updates, Upgrades, other notices and a valid Bitdefender Solution license. The Bitdefender account is mandatory for the use of Bitdefender Solution, as stated in the Documentation.

1.2. For all Bitdefender Solutions, with the exception of Bitdefender Security for AWS, the registration requires a valid subscription key serial number available in the Commercial documentation, from the Bitdefender distributor or reseller from which Customer obtained Bitdefender Solution. This control helps ensure that Bitdefender Solution operates only on validly licensed devices, virtual machines, and mobile devices and that only validly licensed users receive Bitdefender services. The Bitdefender account is necessary for the activation of the online features, as stated in the Documentation.

1.3. For Bitdefender Security for AWS, is a subscription-based service offered by Bitdefender for Amazon EC2 customers.
If Customer purchases directly from Bitdefender, Customer must have an Amazon Payments account with a valid credit card necessary for the monthly billing. Customer is not provided with or required to use a license key.

1.4. Bitdefender Solutions features and terms are presented on the Bitdefender website, e-shop or the applicable Commercial documentation.

1.5. The information given (name, email address, password) during initial setup, will be used as an account name under which Customer may elect to receive services and/or under which Customer may use certain features of Bitdefender Solutions. Customer may change, and Bitdefender strongly recommends Customer to do so, the password at any time after installation of Bitdefender Solutions or activation of the service as may be the case.

2. LICENSE RIGHTS AND RESTRICTIONS

2.1. Upon Bitdefender's acceptance of Customer's order and in consideration of the payment of the fee by Customer and receipt of the corresponding payment by Bitdefender, Bitdefender grants Customer the limited, non-exclusive, non-transferable right to use and/or access Bitdefender Solution that Customer ordered solely for Customer internal business operations, including Customer's Affiliates, and subject to the terms of this Agreement, including the order and the Documentation.

2.2. Customer may allow its Users to use Bitdefender Solutions as per this Agreement and Customer is responsible for their compliance with this Agreement in such use.

2.3. Customer may install or use Bitdefender Solutions and initiate and/or access the services, on as many devices/endpoints as necessary, with the limitation imposed by the total number of licensed seats stated in the order. Depending on the purchased Bitdefender Solution, Customer will be entitled to license for physical computers, endpoints, virtual machines, Amazon EC2 instances and/or Exchange mailboxes, as stated in the purchase orders or other Commercial Documentation. Customer acknowledges and agrees that Bitdefender Solution may be used/configured only on one instance of the console at a time (either on cloud or on premises, but not both at the same time). However, a migration from one console to another is possible, and, to do so, Customer will need to contact Enterprise support for additional details.

2.4. Customer can use one copy of Bitdefender Solution on a single device. If a greater number of copies and/or number of devices or protected resources is specified within the purchase order received from the authorized distributor or reseller (Permitted Number), Customer shall have the right to copy Bitdefender Solution in accordance with such specifications; Customer can make one copy of Bitdefender Solution for back-up or archival purposes. Customer may not exceed the total number of Customer endpoints or servers or protected resources on which all versions of Bitdefender Solution are installed if : a) Bitdefender Solution supports multiple platforms or languages b) Customer receives Bitdefender

Solution on multiple media or c) Customer otherwise receives multiple copies of Bitdefender Solution, or d) Customer receives Bitdefender Solution bundled with other software.

2.5. During the installation process, Bitdefender Solution may uninstall or disable other security products if such products or features are incompatible with Bitdefender Solution.

2.6. If Customer purchases Bitdefender GravityZone XDR for MSP add-on, this requires Threat Intelligence Services (TIS) and Bitdefender Endpoint Detection and Response (EDR) add-ons which will be automatically activated together with Bitdefender GravityZone XDR for MSP add-on and invoiced accordingly.

2.7. Bitdefender Solutions are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Bitdefender Solutions are licensed, not sold. Customer have the right to use Bitdefender Solutions as per the provisions of this Agreement.

2.8. License Restrictions. Under this Agreement, Customer may not transfer or sublicense Bitdefender Solutions to another person or entity; Customer shall not rent, lease, loan, auction, or resell Bitdefender Solutions nor modify, translate, or create derivative works, reverse engineer, de-compile, or disassemble Bitdefender Solutions, in whole or in part, or otherwise attempt to reconstruct or discover the source or object code or underlying ideas, algorithms, file formats, programming or interoperability interfaces (or if the law permits any such action, Customer agrees to provide at least 90 days' advance written notice); Customer shall not use Bitdefender Solutions to provide services to third parties or allow use or access to Bitdefender Solutions by any third party other than contractors or consultants acting on Customer's behalf. Customer may not permit third parties to benefit from the use or functionality of Bitdefender Solutions and Services via a timesharing, service bureau or other arrangement. Customer may not remove any proprietary notices or labels on Bitdefender Solutions and Customer may not disclose results of any program benchmark tests without Bitdefender's prior written consent. If Bitdefender provides Bitdefender Solutions (i) embedded, incorporated, or loaded onto a physical hardware device or (ii) made available to download on a designated physical hardware device, then the license is restricted to use on that device only. Additionally, Customer may not, (a) modify, block, circumvent or otherwise interfere with any authentication, license key or security measures in Bitdefender Solutions b) distribute, license, sublicense, sell, rent, mortgage, encumber, or otherwise transfer or provide a copy of any Bitdefender Solutions (or components thereof including any license or access key or authorization) to any third party; (c) publish, provide, or otherwise make available to any third party, any competitive, performance, or benchmark tests or analysis relating to Bitdefender Solutions without the written permission of Bitdefender which may be withheld or conditioned at the sole discretion of Bitdefender; (d) deploy or use Bitdefender Solutions in any manner other than as expressly permitted in its Documentation; or (h) attempt to do any of the foregoing with regard to a Bitdefender Solutions.

2.9. Customer must obtain all necessary rights and permissions from Customer's Users to use Bitdefender Solutions.

2.10. Customer must check the Commercial Documentation and Bitdefender websites for limitations of usage among the different categories of endpoints.

3. UPDATES

3.1. Customer acknowledges and agrees that, during the Validity Period, a server system of Customer's choice installed in Customer's network may be used for receiving and serving Updates of Bitdefender Solutions. The necessary protocol will not be used for anything other than transmitting and receiving Bitdefender updates of product and signatures files. If Customer does not use a local Update server, Bitdefender offers Customer the possibility to download the updates directly from Bitdefender content delivery network. Some Updates as signature updates, bugfix or smaller updates will be automatically downloaded to Customer's device and major updates will require Customer intervention in the interface.

3.2. Customer must be current in the payment of fees for Bitdefender Solutions or have an active subscription, as applicable, to receive Updates or Upgrades.

4. SPECIAL TERMS AND CONDITIONS FOR THE FOLLOWING BITDEFENDER SOLUTIONS:

4.1. SPECIAL TERMS FOR BITDEFENDER GRAVITYZONE SECURITY FOR EMAIL SOLUTION

4.1.1. Bitdefender GravityZone Security for Email Solution is a 100% cloud-based service that analyzes email traffic and removes unwanted or malicious messages. The service scans all inbound (and outbound) messages for threats including malware and phishing attacks, and examines URLs embedded in messages protecting users from inappropriate or malicious web pages.

4.1.2. Mailbox is defined as the storage location of electronic mail messages found on a remote server or downloaded to the user's device. Email client software typically organizes messages into separate folders including inbox and sent items.

4.1.3. Solution Usage policy:

How is Solution Usage calculated:

The following describes the metrics used to calculate Solution Usage for Bitdefender GravityZone Security for Email during a calendar month. For the avoidance of doubt, a calendar month is calculated from the first to the last day of the month, e.g. January 1st to 31st, April 1st to 30th, etc.

The number of Active Mailboxes meaning shall be: the mailboxes (excluding aliases and distribution lists) that have sent or received at least one email in the period.

For a mailbox to be chargeable, the primary flag must be set to true and the object Class in Active Directory must be user or NULL ("NULL" is included for environments where Active Directory is not used).

Shared mailboxes, Distribution Lists (DLs), resources etc. will have an object Class most commonly
of group or msExchDynamicDistributionList for on-premises or shared mailbox for Office 365 / Exchange Online. These are not counted towards Solution usage.

If Customer is using Azure Active Directory, Customer must grant the correct permissions to allow synchronization of shared mailboxes, otherwise they will be indistinguishable from standard users and subject to billing.

Mailboxes that match the criteria above also need to be Active Mailboxes to be chargeable. An Active Mailbox is a mailbox that has received or sent at least one email message in the period (month).

Usage is the sum of active primary mailboxes as defined above. The Solution usage calculation presented above applies to monthly billing (MSP). For annual or multi-annual billing, the Solution usage is equal to the number of “sold” mailboxes as stipulated in the commercial agreement.

In certain cases, disabled mailboxes may still be subject to billing if they remain in the scan scope of the solution, regardless of mailbox activity status. To prevent billing for such mailboxes, it is recommended to implement a connection rule that excludes listed disabled mailboxes from active scanning. Information on configuring this rule is available in the Bitdefender documentation, specifically under 'Connection Rule Examples.' This exclusion rule helps align the usage with the criteria for 'Active Mailboxes' as defined in herein.

4.1.4. Over-usage. Customer undertakes that the maximum number of Mailboxes that will be subject shall not exceed the number of Subscriptions Customer has purchased from time to time. If the Customer exceeds the number of Subscriptions purchased, the Customer agrees to pay additional Subscription Fees in respect of the additional Mailboxes, backdated to the point of Over usage.

Over-usage shall be usage scenario where an annual/multi-annual paying customer is using more than the number of mailboxes stipulated in the commercial agreement, this being calculated using the Active Mailbox method presented above. Bitdefender reserves the right to invoice the difference between the sold mailboxes and the actual Active Mailboxes, as stated in the Bitdefender Console. Bitdefender reserves the right to suspend Customer account for all licenses.

4.1.5. Bulk email terms and conditions

Note: Security for Email service does not allow for bulk emailing activities that are not compliant with the terms and conditions below.

Users that make use of **Bitdefender GravityZone Security for Email** for sending outbound email must respect the terms and conditions below, pertaining to bulk email. If Customer wishes to send bulk email, Customer and end-users creating the mail shot must comply with the following terms.

Bulk e-mail must be small in size:

- Less than 150KB for less than 100 recipients.
- Less than 30K for less than 1000 recipients.
- Less than 20K for larger than 1000 recipients.
- Email attachments should be posted to a web server, and a link included.

The system can handle up to 300 recipients outbound. If Customer recipient list is larger than 300 email addresses, Customer needs to split the email.

4.1.6. Delivery and Service Level:

Delivery and Service Level agreements do not apply to bulk email. In the event of busy periods, Bitdefender reserves the right to delay the delivery of bulk email as well as reroute it to alternative data centers. Support is not provided for undelivered emails.

Approval - prior to sending

Large campaigns of over 200 recipients must be submitted with a sample email to bulk@bitdefender.info at least 24 hours in advance. Smaller campaigns should *BCC* bulk@bitdefender.info Failure to do this may result in the email being stopped.

Compliance. Customer shall be solely responsible for the compliance with any applicable legislation.

Complaints. If Bitdefender receives abuse complaints, Bitdefender reserves the right to block future campaigns. If Bitdefender receives complaints from a single vendor, Bitdefender is obliged to stop delivery of all email from the Customers' domain to that vendor. (e.g. AOL).

The abuse@yourdomain.tld address must be a valid email address and must be actively monitored.

Sending Limits. All Email Security accounts provisioned starting June 1st, 2021, shall be limited to 600 messages/hour.

4.1.7. GravityZone Security for Email Solution Risks:

It should be noted that email is generally sent unencrypted in clear text and routes through numerous network providers, systems and servers between sender(s) and recipient(s). Each of these providers, systems and servers may have a copy of the complete email message.

The use of Transport Layer Security (TLS) to encrypt server to server transmission of email is becoming increasingly used. There is the option within EMS to use TLS for outbound email with specific domains that support it.

For sensitive messages, including messages containing personal data, the use of a separate email encryption solution is recommended.

It should be further noted that GravityZone Security for Email Solution only covers email sent or received externally. Internal messages sent between users are not processed by Bitdefender.

Scope of Risk: Our staff could access the message body (including file attachments) of email messages sent or received externally - if they are not encrypted - for the short time that they are written to disk and processed in Cloud.
Only a small number of our staff are involved in the administration of EMS systems, or in supporting customers using the service, or those that have access for operational or engineering (software development) reasons have any access to the infrastructure that processes and temporarily stores email messages. The same small number of our staff could access spam messages that are stored in a quarantine if the service is configured to quarantine messages determined to be spam. All service-related data is handled in strict accordance with Data Protection Legislation.

Input data that contains personal data – GravityZone Security for Email Solution: Input data for the GravityZone Security for Email Solution is comprised of inbound and outbound email messages sent or received externally to or from the organization. Email messages are sent unencrypted in clear text unless a separate email encryption solution is used, or TLS is enforced for outbound email sent to a specified domain. Email messages are stored, typically for a few seconds, during analysis and deleted immediately once delivered to Customer email server.

Output data that contains personal data – GravityZone Security for Email Solution:

Ø Output data from the EMS service is comprised of log data relating to inbound and outbound email messages sent or received externally. Log information includes IP addresses, To, From and Subject fields, server responses, and other metadata, but does not include the message body or any file attachments.

Ø Depending on the configuration of the service output data may also include complete email messages that are determined during analysis to be spam messages, if the service is configured to quarantine spam emails rather than delete them. Quarantined messages are stored for thirty (30) days and then deleted.

Ø Log data is held online for ninety (90) days and then archived. Archived log data is deleted after twelve (12) months (but may be downloaded on demand by customers at any time prior to deletion).

4.2. SPECIAL TERMS AND CONDITIONS FOR THE BITDEFENDER GRAVITYZONE SECURITY FOR MOBILE SOLUTION

4.2.1. Bitdefender GravityZone Security for Mobile Solution is a cloud-based service that protects mobile devices against malicious applications, phishing attacks, network threats and device threats. The service consists of a management console on cloud and agent applications on supported mobile device platforms. The service provides a configurable level of protection, which, when configured, scans all inbound (and outbound) browser traffic for phishing threats, analyzes mobile applications, monitors the network traffic and detects operating system and configuration vulnerabilities on mobile devices.

Mobile Device is defined as devices running on Android or iOS (Apple) operating systems.

Chrome Extension is defined as the Security for Chrome extension of Security for Mobile solution that can be installed on chrome browsers. These are also counted as mobile devices.

4.2.2. Solution Usage policy

How is Solution Usage calculated:

The following describes the metrics used to calculate Solution Usage for Bitdefender GravityZone Security for Mobile during a calendar month. For the avoidance of doubt, a calendar month is calculated from the first to the last day of the month, e.g. January 1st to 31st, April 1st to 30th, etc.

a) The number of Active Devices meaning: the devices that have been detected as online (sent or received at least one keepalive message to the management console) in the period. For a device to be chargeable, it must have become online at least once during the period.
b) Without an MDM (Mobile Device Management) integration, it is not possible to detect if an uninstalled / reinstalled device is physically the same device. In these instances, both devices will be charged, being considered as Active Device.
c) On devices where both the mobile agent and chrome extension is installed and enabled at the same time, if the devices are not registered with the same ID to the Security for Mobile console by the MDM (Mobile Device Management) solution, they will be registered as two separate devices on Security for Mobile console and they will be charged as two separate devices. By the time of the release of this document, Google MDM is the only solution tested by Bitdefender that registers the mobile devices and chrome extension as a single device. Please consult with Customer MDM provider to test Customer integration before installing chrome extensions to avoid double billings.
d) Users might decommission old devices and switch to new devices. In such circumstances, rule “a” still applies and they will be treated as two separate devices.
Usage is the sum of active devices (including chrome extensions) as defined above. The Solution usage calculation presented above applies to monthly billing (MSP). For annual or multi-annual billing, the Solution usage is equal to the number of “sold” mobile devices, as stipulated in the commercial agreement.

4.2.3. Over-usage. Customer undertakes that the maximum number of mobile devices that will be subject shall not exceed the number of Subscriptions Customer has purchased from time to time. If Customer exceeds the number of Subscriptions purchased, Customer agrees to pay additional Subscription Fees in respect of the additional mobile devices, backdated to the point of Over-usage.
Over-usage shall be a usage scenario where an annual/multi-annual paying Customer is using more than the number of mobile devices stipulated in the commercial agreement, this being calculated using the Active Devices method presented above. Bitdefender reserves the right to invoice the difference between the sold mobile device subscription and the actual Active Devices, as stated in the Bitdefender Console. Bitdefender reserves the right to suspend Customer account for all licenses.

4.2.4. GravityZone Security for Mobile Solution Risks:

It should be noted that protection capabilities provided by Security for Mobile depends on the admin configuration. By default, “best practices” set of detections are enabled on each new Customer’s account. However, these detections are not designed to take any action on mobile devices. Security admins in charge of managing the mobile security must view the default configurations and enable appropriate actions on their accounts.

Bitdefender Security for Mobile relies on mobile device agent applications to provide protection. However, considering that not all mobile devices are corporate owned, (i.e. BYOD, Bring Your Own Device) the permissions required by the agent to provide the protection configured by

admin might not be approved by the owner of the mobile device, thus, the agents might fail to provide the required level of protection. Asking the end user to provide the required permissions as well as complying with regulations and laws is the Customer's responsibility. We, as Bitdefender, cannot force the end user to provide all the required permissions.

For instance, anti-phishing capability requires a local VPN technology to be enabled on the mobile device. However, enabling this technology requires the permission of the device owner. If such access is not permitted, the anti-phishing technology will not work as intended.

For easier compliance with regulations and laws, security admins can alter the level of data to be collected from the mobile devices via mobile agents. Please note that limitations in data collection can also lead to not being able to utilize some of the capabilities. For instance, deep analysis capability requires access to the apk files on Android devices. An admin can choose to not collect application binaries on mobile devices (or a set of mobile devices). However, when application binary collection is disabled, the deep analysis capability cannot be utilized for the applications on those mobile devices.

4.3. SPECIAL TERMS FOR BITDEFENDER INTEGRITY MONITORING ADD-ON

4.3.1. Bitdefender Integrity Monitoring add-on reviews and validates changes made on Windows and Linux endpoints to assess the integrity of multiple entities as described in the documentation of the Solution. Integrity Monitoring add-on operates based on default rules, provided by Bitdefender, and custom rules. These rules are available in the **Policies** > **Integrity Monitoring Rules** page of Control Center. Based on these rules, Integrity Monitoring add-on takes action when events are generated for files, folders, registry entries, users, services and installed software. These events are displayed on the **Reports** >**Integrity Monitoring Events** page of Control Center.

4.3.2. During maintenance window performed with Bitdefender Patch Management, Integrity Monitoring default rules will be suspended according to the documentation. For clarity, this means that if no policy application or reapplication occurs while Integrity Monitoring is suspended, the old attributes of entities present in alerts after resuming Integrity Monitoring are the ones that were present before the patching process started. If a policy application or reapplication occurs while Integrity Monitoring is suspended, the old attributes are going to be renewed to the ones present for monitored entities at the time of application or reapplication.

4.4. SPECIAL TERMS FOR BITDEFENDER GRAVITYZONE CLOUD SECURITY

4.4.1. Bitdefender Gravityzone Cloud Security module provides access to an all-in-one platform encompassing CIEM (management of identities and access, identification of risks dynamically) and CSPM (Security and Compliance and regulatory best practices and frameworks, assessment of misconfigurations).

4.4.2. The Cloud Security Posture Management (CSPM), which is a continuous management of IaaS and PaaS security posture through prevention, detection, and response to cloud infrastructure risks, applies common frameworks, regulatory requirements and enterprise policies to proactively and reactively discover and assess risk/trust of cloud services configuration and security settings.

4.4.3. The scope of such management is to verify if there are issues, and if one is identified, to provide remediation options (automated or human-driven). Bitdefender Gravityzone Cloud Security provides Customer with the possibility to identify and zoom in on a suspected asset and understand the full context from both a configuration and activity perspective with associated event severity, thereby reducing time in detecting, investigating, and remediating threats.

4.4.4. Bitdefender Gravityzone Cloud Security scanner has hundreds of rules and counting across different standards. Each rule is complete with an appropriate risk value, description, and remediation instructions that may include the option to execute a one-click or playbook remediation. Bitdefender's ruleset also identifies when Customer contravenes security best practices, alerting Customer when they happen so that Customer can prioritize these fixes accordingly.

With continuous visibility across cloud resources from a single console Customer can enforce configuration guardrails with hundreds of fix misconfigurations before they lead to security incidents.

4.4.5. Customer may use the Bitdefender Gravityzone Cloud Security and initiate the solution within the limitation imposed by the total number of billable resources as defined in the Documentation and stated in the purchase order. If Customer has more billable resources in Customer environment than the number of billable resources Customer has purchased, Bitdefender will restrict the solution and scan to the limited number of billable resources stated in Customer order; Please note that Customer may add more billable resources with a new order.
For the avoidance of any doubt, the Bitdefender Gravityzone Cloud Security may not be used/configured on more than one instance at a time.

EXHIBIT B - SPECIAL TERMS AND CONDITIONS FOR MDR SERVICES AND CYBERSECURITY WARRANTY SERVICE

1. SERVICES DESCRIPTION

1.1. Prerequisites. Service Setup Phase. For using MDR Services, Customer needs to have a valid activated license to a Bitdefender Solutions and a valid MDR Services subscription.

1.2. Onboarding, Deployment & Configuration

The onboarding process is deemed finalized when Customer or Customer Contractor (i) have enabled MDR Services for Customer or a User in GravityZone, (ii) installed and enabled Bitdefender solution on all endpoints, and (iii) Customer has set up Emergency Contacts, Pre-approved Actions, and Notifications preferences in the MDR Portal ("Onboarding").

Onboarding is followed by Deployment & Configuration phase, in which Customer or Customer Contractor is responsible for deploying, installing, and configuring the endpoint detection and response feature and the extended detection and response integrations in the GravityZone console. Bitdefender shall have no liability towards Customer with respect to the Pre-approved Actions and / or their consequences.

Note that for certain MDR Services, according to the specifications in the Documentation related to the respective service may include Professional Services support, during the Solution Setup Phase. The provision of the Professional Services support needs to be stated in the Commercial Documentation.

1.3. Active 24/7 Monitoring Service Delivery Phase

a) Monitoring potential attacks: Only after the completion of the Solution Setup Phase, devices having the GravityZone agent installed shall be monitored, as per reasonable commercial diligence, 24x7 during the Validity Period. However, the parties acknowledge and agree that interruptions may occur outside of Bitdefender's control, such as those due to internet provider outages and the like.

b) Notifications and Updates. Once a security incident has been identified in Customer environment, which could be either of the following cases: i) an attacker is active on a device conducting malicious activity, ii) successful malware installation or iii) vulnerability exploitation that leads to additional activity on the endpoint ("Incident"), Bitdefender will provide an initial notification through the agreed communication contacts provided by Customer or Customer Contractor and provide subsequent updates in the following timeframes based upon our determination of the applicable severity level. Bitdefender will notify and update Customer or Customer Contractor through agreed communication channels depending upon the severity of the situation and consistent with any procedures that have been established and documented with Customer. The notification times stated below start from the moment when MDR Services has: i) identified a potential Incident, and/or (ii) if the case, requested for more information from Customer or Customer Contractor. For the avoidance of any doubt, Bitdefender shall use all commercial reasonable efforts to notify Customer or Customer Contractor as stated in the below response timetable, which does not apply until Customer or Customer Contractor receives notice that an Incident has occurred, and that Bitdefender has assigned the said incident a severity level.

Critical and High priority severity levels are not available for non-production systems. Customer hereby acknowledges and agrees that Bitdefender may add additional notification methods in the future.

Service Level Agreements (“SLAs”):

Service Level (example incidents)	Initial Notification (from event identification)	Update Frequency (after Initial Notification)
Critical Advanced or Interactive Attacker. Advanced Persistent Threat (APT): Nation-State Threat Group or Advanced Cyber-Crime Organization. Data staged for exfiltration. Confirmed data exfiltration.	30 Minutes	Every Hour
High High confidence intelligence-driven detections. Command line activity spawned by a suspicious process. Web exploits. Privilege escalation. Credential theft.	30 Minutes	Every Hour
Medium		

High confidence known malware. High confidence malicious document. Social engineering of binary files.	Notification Not Required. Recommendation is posted in the MDR Portal	Notify Customer if mitigation recommendations require Customer approval.
Low Low confidence known malware (commodity malware or adware) Low confidence malicious documents Command line activity used for common administrative purposes and lateral movement or reconnaissance activity	Notification Not Required. Recommendation is posted in the MDR Portal	Notify Customer if mitigation recommendations require Customer approval.

For Customer's MPSs: MSPWILL RESPECT THE ABOVE-MENTIONED SLA FOR NOTIFYING THEIR CUSTOMERS AND FOR RESPONDING BACK TO BITDEFENDER REPRESENTATIVES. BITDEFENDER WILL NOT BE HOLD LIABLE FOR ANY CLAIMS OR LOSSES RESULTED FROM BREACHING THE SLAs OF NOTIFING AND RESPONSE BY CUSTOMER CONTRACTORS.

c) Alert review and validation initiated by Customer: Customer can access Support channels 24x7 and inquire about the validity of an incident seen by Customer in GravityZone. Customer or Customer Contractor will be notified through agreed communication channels that the investigation request has been received, and the investigation has started. Bitdefender can ask for additional information if needed for the assessment. Once an investigation has been concluded, Customer or Customer Contractor will be notified of the completion of the investigation.

NOTE: Forensic analysis of the attack is not included in the MDR Services

1.4. Reporting

MDR Services will provide standard information and reports to Customer or Customer Contractor as part of normal business operations including the following types of reports in Customer covered environment:

Realtime Dashboard for Users – A summary of all security events seen in Customer covered environment over the last day, week, or month.

Monthly Report – Monthly reports include a summary of all security events seen in Customer covered environment for the previous month, including threat hunting and incident summaries.

Flash Report – The Flash reports generated immediately after incidents are provided to provide Customer with initial findings and containment actions taken, if applicable.

After Action Report – After Action Reports are generated for completed incident investigations. They contain the complete details of the attack, a summary of the actions taken and any recommendations on changes in the Environment to help prevent similar incidents in the future.

1.5. Responses to live attackers

Bitdefender can identify whether there is an attack or not and Customer can decide how Bitdefender is to react, as per the Pre-Approved Actions (PAAs) that Customer or Customer Contractor have previously envisaged. PAAs are enabled by default but can be toggled on or off directly in the MDR Portal (please find herein the relevant location: bitdefender.com/business/support/en/124809-151519-pre-approved-actions.html). Please note that turning off a PAA will inhibit timely actions by Bitdefender. In addition, Customer understands and hereby expressly allows and agrees that Bitdefender shall be entitled to create a remote shell on devices to further investigate or limit the impact of attacks. The ability to create a remote shell is essential to the MDR Services, and its main purpose is to obtain otherwise unobtainable necessary information during an investigation and to properly contain attackers. All actions performed by an analyst via remote shell are stored in the GravityZone console for Customer to audit. Customer hereby expressly authorizes any activity taken by the Bitdefender analyst while the remote shell feature is used, provided however that such activity will be limited to the purpose of providing MDR Services. Additional information on remote shell sessions and SOC may be found here: https://www.bitdefender.com/business/support/en/77209-151142-edr-investigating-incidents.html.

For the avoidance of any doubt, Bitdefender shall be entitled to perform (i) the PAAs previously detailed and explained to Customer, both with respect to the timeframe for taking such action(s) as well as with respect to all consequences of taking the said actions (including unforeseen consequences which Customer hereby expressly agrees upon); (ii) any other action that Customer expressly authorizes, once Customer or Customer Contractor have been notified with respect to an incident. In addition, Customer expressly acknowledges and agrees that Bitdefender has no obligations (including no liabilities and no damages payment) towards Customer (nor towards MSPor any of its Users) for any and all repercussions in connection with taking any of the (i) or (ii) actions, provided that Customer express consent was previously obtained, except, for Users, in the case of usage of remote shell feature.

1.6. Delivery Channels

Bitdefender may choose to provide MDR Services using the following delivery channels: phone, email or remotely accessing Customer GravityZone Console. During the delivery of MDR Services, Bitdefender may, at its sole discretion and without any obligation, capture MDR Services sessions in different forms (such as, but not limited to voice recording, written recording, database monitoring) for quality improvement purposes and/or market research purposes. Customer agrees to allow Bitdefender to perform such captures, including recordings of any type and to use and process any information resulted from such recordings for MDR Services improvement purposes, for marketing research or training purposes and in order to respond to any legal or regulatory requirements, in compliance with the applicable laws.

1.7. MDR Services Availability

Bitdefender will make operationally and commercially reasonable efforts to make MDR Services available on a 24x7basis. However, MDR Services delivery may be limited to some geographic regions or may suffer interruptions due to technical maintenance or Internet provider issues, independent of Bitdefender's control. Customer agrees to grant Bitdefender's representatives the following rights: (i) to use whatever support or remote access tools are necessary to investigate the incident(s); (ii) to install Bitdefender proprietary or third party licensed remote access tools, for the sole scope of providing MDR Services; (iii) to access Customer computer remotely and modify settings and configurations, including installing or removing specific items, in order to solve a problem or diagnose more complex problems, either as a result of a pre-approved action or as a direct response to Customer indications; (iv) to gather data from Customer / its devices only for the purpose of providing MDR Services and as a part of problem diagnosis process.

As a result of using MDR Services, including specific MDR Services support sessions, Bitdefender can remove any remote access tools software installed on Customer / its End Customer computer for the scope of providing MDR Services; however, by signing the present Agreement, Customer is informed and expressly accepts the fact that there might be residual files left on Customer computer as a consequence of usage of the support and/or remote tools.

In addition, it is Customer sole responsibility to check whether any residuals impact Customer in any way and to resolve any and all potential consequences of such residuals. Bitdefender hereby accepts no liability whatsoever with respect to any residuals.

For MDR Services requiring user accounts, only the single individual user assigned to a user account may access or use it. Customer is liable and responsible for all actions and omissions occurring under Customer and Customer user accounts for MDR Services.

1.8. Prerequisites for MDR Services and Warranty.

During the Validity Period, so long as the Customer also subscribes to the GravityZone Platform in compliance with the Master Agreement, the GravityZone Platform which will screen for any Ransomware shall provide cybersecurity services. The Customer acknowledges and agrees that the functionality of the services can be affected if at least following security measures are not implemented:

a. The GravityZone Platform and endpoints are deployed in accordance with the Documentation and such endpoints are currently active and properly configured;

b. Each XDR sensor is deployed and configured according to the GravityZone Product Documentation, if the Customer has purchased the corresponding XDR license.

c. The GravityZone Platform and all Endpoints of the Customer have the following required configurations and attributes:

i. **GravityZone Platform**:

· Antimalware On-Access module is enabled, cloud-based threat detection is enabled, advanced threat detection module is enabled and set on normal or aggressive mode (see Documentation for details), fileless attack protection module is enabled, ransomware mitigation module is enabled and monitors both locally and remote shares, hyperdetect module is enabled and all its protection levels are set to normal or aggressive, the advanced anti-exploit module is enabled and it's configured to block memory access for lsass attacks and kill processes in case of privilege escalations, the sandbox analyzer module is enabled and configured to prefilter content in an aggresive mode (see Documentation for details).

· Network protection module is enabled, and scan SSL is enabled, the antiphising module is enabled, web and email traffic scanning is enabled, network attack defense is enabled, and all attack techniques are enabled and the action taken is block.

· The firewall module is enabled.

· The remote shell module is enabled.

· The EDR module is enabled.

· All MDR Services pre-approved actions are enabled.

· The Customer has provided at least one valid Emergency Contact in the MDR Portal.

· Two-factor authentication is enabled in the Management Console, or Single Sign On with two-factor authentication, enabled and enforced for all Management Console users.

· Agent is not tampered intentionally by Customer, and it is at its latest version also available on Bitdefender update servers.

ii. **Operating system**:

· The Services applies to Standard (not Legacy) Windows, Linux and MacOSX Agents, and on supported versions of Microsoft Windows (as specified in the GravityZone Product Documentation).

· Each Endpoint is malware-free prior to GravityZone Agent installation.

· The OS is fully updated and patched for security updates on each covered endpoint, and all vulnerable applications are updated to the latest releases.

1.9. Professional Services

Professional Services will commence on a mutually agreed upon date as stated in a SOW signed by the parties. Estimates provided for Professional Services performed on a time and material basis are estimates only and not a guaranteed time of completion. Professional Services performed on a fixed fee basis are limited to the scope of services stated in the SoW.

Professional Services do not constitute "works for hire," "works made in the course of duty," or similar terms under laws where the transfer of intellectual property occurs on the performance of services to a payor. The only deliverable arising from the Professional Services is a report consisting primarily of the findings, recommendations, and adversary information. Customer owns the copy of the report (including without limitation, all Customer Confidential Information therein) delivered to Customer ("Deliverable"), subject to Bitdefender's ownership of the Bitdefender Materials. Customer agrees that relative to Customer, Bitdefender exclusively owns any and all software (including object and source code), flow charts, algorithms, documentation, adversary information, report templates, know-how, inventions, techniques, models, ideas and any and all other works and materials developed by Bitdefender in connection with performing the Professional Services as well as the trademark Bitdefender (including without limitation all intellectual property rights therein and thereto) (collectively, the "Bitdefender Materials") and that title shall remain with Bitdefender. For the avoidance of doubt, the Bitdefender Materials do not include any Customer Confidential Information, or any other materials or data provided by Customer. Upon payment in full of the amounts due hereunder for the applicable Professional Services and to the extent the Bitdefender Materials are incorporated into the Deliverable(s), Customer shall have a perpetual, non-transferable, non-exclusive license to use the Bitdefender Materials solely as a part of the Deliverable(s) for Customer Internal use only.

1.10. Cybersecurity Warranty Service.

Bitdefender provides a limited Cybersecurity Warranty Service for Customers that have a fully paid-up subscription for MDR Services and have a currently supported version of the MDR Services correctly installed and fully operational on their endpoint(s) for certain type of MDR Services as mentioned on Bitdefender websites and only if stated in its Commercial Documentation (the "**Warranty**"), in accordance with the terms and conditions governing the Cybersecurity Warranty Service provided in Appendix A below (the "**Warranty Agreement**").

2. Rights of Usage

2.1. Subject to the terms and conditions of this Agreement, Bitdefender grants Customer a limited, non-exclusive, non-transferable right to access and use MDR Services in accordance with any applicable Documentation solely for Customer's internal use during the applicable

Validity Period. The internal use will be limited to access and use by Customer employees, Customer's Affiliates' employees and Customer's Contractors in either event, solely on Customer behalf and for Customer benefit. For clarification purposes, internal use does not include access or use: (i) for the benefit of any person or entity other than Customer or Customer's Affiliates or (ii) in any event, for the development of any product or service. Customer access and use is limited to the quantity in the applicable Order.

Customer may allow its Users to use MDR Services as per this Agreement and are responsible for their compliance with this Agreement in such use.

During the installation process, MDR Services may uninstall or disable other security products if such products or features are incompatible with Bitdefender Solution.

2.2. Customer agrees to use MDR Services in accordance with laws, rules and regulations and acknowledges that Customer is solely responsible for determining whether a particular use of MDR Services is compliant with such laws. Customer must obtain all necessary rights and permissions from Customer Users to use MDR Services.

Customer is liable and responsible for all actions and omissions occurring under Customer and its Customers' user accounts.

3. Usage Restrictions

3.1. Customer will not use MDR Services (or any portion thereof) to: (i) alter, publicly display, translate, create derivative works of or otherwise modify Bitdefender Solutions and Services ; (ii) transfer, distribute or otherwise transfer Bitdefender Solutions and Services to any third party, or employ or authorize a third party to use, benefit or view the MDR Services, or to provide management, hosting, or support for an MDR Services, except as expressly permitted herein; (iii) allow third parties to access or use Bitdefender Solutions and Services except for as expressly permitted herein; (iv) create public Internet links to MDR Services or frame or mirror any MDR Services content on any other server or wireless or Internet-based device; (v) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for Bitdefender Solutions and Services (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to MDR Services or its related systems or networks; (vi) use MDR Services to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (vii) remove or alter any notice of proprietary right appearing on Bitdefender Solutions and Services; (viii) conduct any stress tests, competitive benchmarking or analysis on, or publish, provide any performance data of MDR Service; (ix) cause, encourage or assist any third party to do any of the foregoing.

Appendix A – Bitdefender Terms and Conditions for Cybersecurity Warranty Service ("Warranty Agreement")

Bitdefender provides this limited Cybersecurity Warranty Service (the "**Warranty**"), on the terms and conditions outlined herein in the **Warranty Agreement,** for Customers that have a current, fully paid-up subscription for MDR Services and have a currently supported version of the MDR Services correctly installed and fully operational on their endpoint(s). Customer hereby agrees to have read, to have understood, and to be bound by this Warranty Agreement.

This Warranty is a third-party service provided by Cysurance under the Cysurance Certification Warranty Program Terms and Conditions provided below ('**Cysurance T&C**).

This Warranty is part of Bitdefender Services and is subject to the Master Service Agreement for Bitdefender Business Solutions and Services (the "**Agreement**"). In the case of conflict between these documents in respect of the Warranty, then the terms of the Agreement and the Cysurance T&C provided herein shall prevail over the Agreement to the extent of such conflict.

Capitalized terms not defined in the Cysurance T&C shall have the meaning given to them herein below or in the Agreement.

1. Definitions

1.1. "**Compliant Setup**" means Customer's endpoint environment using a current supported operating system that is free of known malware and/or viruses at the time immediately prior to the Qualifying Event, and such environment has an overall risk score less than 30% as indicated by the Executive Summary Dashboard in the GravityZone Platform and all endpoints from the Customer's environment are managed and updated to latest Bitdefender Endpoint Security Tools version.

1.2. "**Warranty Term**" means the time period in which Customer (i) has a current, fully paid-up MDR Subscription and (ii) runs a currently supported version of the Bitdefender Solution correctly installed, configured and enabled to the recommended settings on all of the managed endpoints in compliance with the MDR Services Description, the relevant Documentation, Prerequisite Terms, and the terms and conditions of this Warranty.

2. Warranty

2.1. The Warranty is available to a Customer in respect of its Managed Endpoints. The Warranty does not apply to MSPs, or Customers of MSP and it is non-transferable. The Warranty is only available to a current subscriber of the MDR Services as stated on Bitdefender website or MDR PLUS service where the Customer has purchased a subscription. For the avoidance of doubt, a Customer that has an MDR Foundations, MDR Premium or MDR Enterprise subscription is not entitled to the Warranty until such Customer renews its Subscription. Only Customers that purchase the MDR Subscription for less than 1000 Endpoints in their environment are eligible to get a Warranty subscription included in the MDR Subscription price. Customers that purchase an MDR PLUS subscription or an MDR Subscription but for more than 1000 Endpoints in their environment are eligible to get a Warranty PLUS subscription.

2.2. If, prior to the scheduled renewal date, an Existing Customer (a) increases the Use Level of its Subscription license for MDR and (b) did not purchase the Warranty but would like to add it to the existing MDR Subscription, then the Warranty will apply to their entire augmented Subscription.

2.3. The Warranty is provided AS IS and may be modified at any time at the sole discretion of Bitdefender, and only the then current version of the Warranty as published by Bitdefender shall apply.

2.4. This Warranty is not intended to and shall not be construed to give any third party any interest or rights (including, without limitation, any third-party beneficiary rights) with respect to or in connection with any agreement or provision contained herein or contemplated hereby. Only the Customer has the right to enforce this Warranty.

2.5. THIS WARRANTY MAY BE CANCELLED, SUSPENDED OR REVISED BY BITDEFENDER BY REASONABLE WRITTEN NOTICE AT ANY TIME AND AT BITDEFENDER'S SOLE DISCRETION. SUCH NOTICE MAY INCLUDE A POSTING TO BITDEFENDER WEBSITE OR A BANNER ON THE GRAVITYZONE CONSOLE.

2.6 THIS WARRANTY DOES NOT AND SHALL NOT BE DEEMED TO PROVIDE A CONTRACT OF INSURANCE UNDER ANY LAWS OR REGULATIONS AND SHALL BE NULL AND VOID IN ANY COUNTRY OR JURISDICTION IN WHICH IT IS DEEMED TO BE A CONTRACT

OF INSURANCE OR AN OFFERING OF INSURANCE.

3. SERVICES DESCRIPTION:

3.1. **Prerequisites**. Service Setup Phase. For Users: For using the Warranty, Customer needs to have a valid MDR Services subscription.

3.2. Onboarding Process. Upon the Customer's purchase of the Cysurance add-on as part of their Bitdefender Managed Detection and Response (MDR) service, the following onboarding process shall apply:

3.2.1 Acceptance of Terms and Conditions. The Customer must accept the Bitdefender Warranty Agreement which includes the Cysurance Warranty Terms and Conditions before gaining access to the MDR Portal following the purchase of the Warranty. This acceptance is a prerequisite for accessing the MDR Portal, and the Customer will be prompted to agree upon their next login. The Warranty activation is independent of the Customer's acceptance of the Warranty Agreement and the Cysurance Warranty Terms and Conditions.

3.3. Activation of Cybersecurity Warranty Service. The Cysurance Warranty ("Warranty") shall commence concurrently with the activation of the Customer's MDR license at the Start Date. The Start Date of the Warranty will be displayed within the Bitdefender MDR Portal and Bitdefender GravityZone Portal.

3.4 Validity of the Cybersecurity Warranty Service. The Customer acknowledges that the Warranty Validity Period is tied to the MDR Service Validity Period and will not exceed the term of the MDR Service unless renewed.

3.5. Integration and Data Handling. The Customer data will be integrated with the Cysurance API for the purposes of warranty registration and management. Bitdefender will securely store the Cysurance token along with details such as the start and end date of the Warranty, the tier of the Warranty, and the country of coverage.

3.6. Communication of Cybersecurity Warranty Service Activation. Upon activation of the Warranty, the MDR Portal will send an email notification to the Customer, which shall include the Start date of the Warranty, the tier of the Warranty, and a link to the Warranty page within the MDR Portal for further guidance.

3.7. Cancellation, Renewal and Continuity. The Warranty continues monthly until expressly canceled, or upon termination of the Customer's MDR Service Agreement, whichever comes first. In the event of a renewal of the MDR Service Agreement, the Customer must re-accept the Warranty Agreement. If the MDR Service Agreement is renewed after expiration, the Warranty will be treated as a new subscription and subject to the onboarding process outlined in this section.

3.8. Termination and Expiration. Upon the expiration or termination of the Customer's MDR Service Agreement, the associated Warranty will also be terminated. The MDR Portal will notify the Customer via email that their Warranty has ended.

4. Claims Process

In the event of a loss covered under the Warranty Agreement, the Customer may submit a claim by following the procedures outlined in the Warranty documentation provided within the MDR Portal. Upon submission of a claim, the following process and Service Level Agreement (SLA) shall apply:

4.1. Submission of Claim. How to file a claim

If the Customer believes it is eligible for reimbursement, he must notify Cysurance within 48 hours of learning of a company-triggered event using the claim form from the link on the Warranty page in his Bitdefender MDR Portal. All reimbursements require prior approval from Cysurance, Bitdefender's warranty partner, so the Customer must file the claim immediately upon discovery.

4.1.1. Notify Cysurance within 48 hours of the incident discovery.

Customer must notify Cysurance within 48 hours of learning of a company-triggered event. In the event of a claim, Cysurance recommends notifying Cysurance as a priority, as claims for reimbursement require prior approval.

4.1.2. Provide Cysurance with information about the incident, the strain of malware or data logs with associated traits for a device, and covered software affected.

Proof of breach is required when submitting a claim for reimbursement. The affected endpoints' log data or supporting evidence will be required for validation. This needs to be electronic records that evidence the breach. Most of the time this will be in one of the victims' log files, but if logs are not available, then screenshots and other types of recordings may be sufficient.

4.1.3. Verify that the covered software was current with all system patches and updates before the incident.

As a best practice, Customer must follow a patching cadence with commercially reasonable measures taken - respectively close to the latest patch cycle release. In the event of a claim, Cysurance may request confirmation of activated licenses and the version update of the covered software.

Bitdefender Cybersecurity Warranty Service will not respond to a systemic failure of the service provider infrastructure, of an application, or of software that results in a loss for Customer company.

4.1.4. Customer needs to check the Warranty Service Enrollment Prerequisites at art 5 below.

4.1.5. Provide an itemized invoice to Cysurance of the services performed to remediate the incident (not to exceed $150/hr).

This applies in case the Customer intends to use services from a third party to assist with the remediation for Customer company. Approval from Cysurance for reimbursement will be required prior to engagement or invoices submitted.

4.1.6. Respond promptly to any requests related to the incident, diagnosing and servicing of the covered software, and follow any instructions provided by Cysurance.

The case incident will be closed within 15 days in the event of insufficient verification data or lack of response. Cysurance shall provide prior written notice.

The customer is entitled to a maximum of 1 valid event claim per year.

Remember to provide Cysurance with available supporting information when reporting claims.

In order to file a claim, complete the Warranty Service Claim Form online by using the Warranty page in the MDR Portal.

4.2. Acknowledgment. The Customer must submit the claim through the designated claim form available on the Warranty page within the MDR Portal. Upon submission, Cysurance shall acknowledge receipt of the claim within 12 (twelve) hours confirming the claim's receipt and initiating the review process.

4.3. Initial Review and Preliminary Response. Within 5 days of acknowledging receipt, Cysurance shall conduct an initial review of the claim based on information provided at that time. During this period, Cysurance will provide the Customer with a preliminary response, indicating, when possible, under the circumstances and information available, whether the claim is eligible under the Warranty and outlining any additional information or documentation required from the Customer.

4.4. Claim Resolution. After receiving all requested information and documentation from the Customer, and if such information and documentation is received from the Customer, Cysurance shall endeavor to resolve the claim within 5 business days. The resolution of the claim may involve assessment, review, approval and processing of services provided as well as submitted invoices, the requested compensation, denial **of** the claim, or further investigation if required. The Customer will be promptly notified of the outcome, along with any actions taken or required.

4.5. Customer Support and Communication. Throughout the claims process, the Customer shall have access to support from the Bitdefender Customer Success Team and Cysurance Concierge Team. Inquiries related to the claim will be addressed within 48 hours, during normal business hours. The Bitdefender Customer Success Team and Cysurance Concierge Team will work collaboratively to ensure the Customer is informed and supported throughout the process.

4.6. Escalation and Dispute Resolution. If the Customer experiences delays or disputes the handling of their claim, they may escalate the issue to Cysurance dedicated claims manager. The escalated issue will be reviewed and addressed within 5 business days of the escalation request. Both Cysurance and Bitdefender are committed to resolving escalated issues in a fair and timely manner.

4.7. Limitation of Liability. Cysurance is the primary entity responsible for processing and resolving claims under the Warranty. Bitdefender's role is limited to facilitating communication, assisting with the provision of information and materials on behalf of Customer, and providing support with the Enrollment. Bitdefender shall not be liable for any delays, failures, or actions by Cysurance that affect the claim process, except where such delays or failures are directly attributable to Bitdefender's actions or omissions.

This Claims Process and SLA are designed to ensure that the Customer's claims under the Cybersecurity Warranty Program are handled efficiently and transparently, providing timely resolution and support throughout the process.

Pre-existing Events. This limited Warranty does not extend to pre-existing Events, meaning any unauthorized access to Customer's endpoint environment that occurs before Customer's Warranty Term.

5. Cybersecurity Warranty Service Enrollment Prerequisites

5.1. Enrollment Prerequisites

The Bitdefender MDR Cybersecurity Warranty Service ("Warranty") only provides financial reimbursements when cyber controls are in place, so it's important to ensure that Customer meets the minimum best practice cybersecurity controls to qualify for enrollment.

5.1.1. The Customer deploys industry standard and up-to-date anti-virus or comparable prevention tools on its endpoints.

All events must be verified through log or event data. Supporting evidence and log data for the affected endpoints are required when filing reimbursement claims.

5.1.2. PHI encryption and Data backups are in place for the Customer.

PHI encryption only applies to companies regulated by HIPAA. Data backup is mandatory for all Customers. A solution that encrypts data at rest and regularly scans for viruses and malicious data is required. Cloud backup solutions are also acceptable if they meet the above criteria.

5.1.3. multi-factor authentication is active on all Customer email accounts.

Multi-factor authentication is essential, as it makes stealing information harder for the average criminal. MFA prevents bad actors from gaining access to a network via a stolen password and, in doing so, allows other security tools to function as designed.

5.1.4. The Customer performs commercially reasonable maintenance, including applying patches and updates within 60 days of release.

As a best practice, the Customer must follow a patching cadence with commercially reasonable measures taken – respectively close to the latest patch cycle release.

5.1.5. The Customer must offer security awareness training to its employees.

All employees should receive security awareness training to ensure they have the skills required to identify an attack. If the Customer requires security awareness training, he must contact Bitdefender for assistance.

5.1.6. Out-of-cycle wire transfers and invoice routing information changes must be verified with the request and documented.

Business controls that document any change request to invoice routing and wire transfers are required, and documentation must be made available in the event of an attack.

5.1.7. The Customer applies his best efforts towards data privacy and is compliant with any required regulatory conditions.

If applicable, Customers must adhere to any national, state, federal, and/or regulatory, privacy, and security policies related to which they are subject, including, but not limited to, PCI, HIPAA, and SEC standards.

For Customers regulated under HIPAA/PCI/SEC/OSHA:

- An annual risk assessment is completed and documented.

- PHI was inventoried and accounted for before the incident.

- All employees completed HIPAA training before the incident and within the past 12 months.

5.2. Warranty. During the Warranty Validity Period, so long as the Customer also subscribes to the GravityZone Platform in compliance with the Agreement, **for the cybersecurity services to the Customer's endpoints thought the Bitdefender GravityZone Solution having activated the protection for Ransomware on its endpoint ("Endpoints").** The Warranty granted herein shall apply to all such endpoints provided that:

a. The GravityZone Platform and endpoints and MDR subscription are deployed in accordance with the Documentation and such endpoints are currently active and properly configured;

b. Each XDR sensor is deployed and configured according to the GravityZone Product Documentation, if the Customer has purchased the corresponding XDR license. Only Files that are on Endpoints are covered under this Warranty;

c. The GravityZone Platform and all endpoints of the Customer have the following required configurations and attributes:

i. **GravityZone Platform**:

· Antimalware On-Access module is enabled, cloud-based threat detection is enabled, advanced threat detection module is enabled and set on aggressive mode (see Documentation for details), fileless attack protection module is enabled, ransomware mitigation module is enabled and monitors both locally and remote shares, hyperdetect module is enabled and all its protection levels are set to aggressive, the advanced anti-exploit module is enabled and it's configured to block memory access for lsass attacks and kill processes in case of privilege escalations, the sandbox analyzer module is enabled and configured to prefilter content in an aggresive mode (see Documentation for details).

- Network protection module is enabled, scan SSL is enabled, the antiphising module is enabled, the web and email traffic scanning is enabled, the network attack defense is enabled, and all attack techniques are enabled and the action taken is block.

- The firewall module is enabled.

- The remote shell module is enabled.

- The EDR module is enabled

- All Bitdefender MDR Service pre-approved actions are enabled.

- Customer has provided at least one valid Emergency Contact in the MDR Portal

- Two-factor authentication is enabled in the Management Console, or Single Sign On with two-factor authentication, enabled and enforced for all Management Console users.

- Agent is not tampered with intentionally by Customer, and it is at its latest version also available on Bitdefender update servers.

ii. **Operating system**:

- The Warranty applies to Standard (not Legacy) Windows, Linux and MacOSX Agents, and on supported versions of Microsoft Windows (as specified in the GravityZone Product Documentation).

- Each endpoint is malware-free prior to GravityZone Agent installation.

- The OS is fully updated and patched for security updates on each covered endpoint, and all vulnerable applications are updated to the latest releases.

d. The Customer adheres to the following manual actions post infection (i.e., upon discovery of Ransomware):

- Immediately (no more than an hour upon discovery) adds the specific Ransomware threat to blacklist;

- In case the Ransomware was not blocked but only detected – takes a remediation and rollback action within 1 hour of infection/discovery of the Ransomware; and and Notifies Cysurance of the Ransomware discovery within 48 hours at Cybersecurity Warranty Service Claim Form online by using the Warranty page in the MDR Portal.

Pre-existing Events. This limited warranty does not extend to pre-existing Events, meaning any unauthorized access to Customer's endpoint environment that occurs before Customer's Warranty Term.

ANNEX 1 TO APPENDIX A

Cysurance Terms:

Cysurance Certification Warranty Program Terms and Conditions

This Annex 1 is a part of the Subscriber General Terms and Conditions Agreement (the "***Agreement***") to which this Annex 1 is attached. The Cysurance Certification Warranty Program will provide Participants with a warranty in respect of (1) the Cysurance vetted and approved external monitoring software products Participants license from Prime Subscriber (the "***Warrantied Software Systems***"), and (2) the ongoing services delivered by Cysurance as set out below (collectively, the "***Warrantied Software System/Services***"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Appendix A above.

1. Definitions.

a. BEC Event means a business email compromise (BEC). The Certification Warranty applies to a BEC Event which is a full, unauthorized threat-actor takeover of a Participant account in its Environment that is monitored by Solutions implemented by Prime Subscriber. The Certification Warranty does not apply to incidents where the social engineering of an individual acting on behalf of or with the Participant has resulted in lost income, lost funds or other fraud of Participant. To be a Qualifying Event, a BEC Event must result from the compromise of credential or other unauthorized access in and of a Participant's own Environment. As an example, where a Participant's HVAC vendor is compromised, and an unauthorized third-party uses quality of the HVAC vendor to persuade the Customer to send funds to an unauthorized recipient, such is not a Qualifying Event, as the compromised environment is not Participant's, but belongs to its HVAC vendor.

b. Benefit End Date means the last day of Participant's qualifying Subscription Term (or other applicable Solutions Agreement), or any qualifying renewals thereof.

c. Benefit Start Date means the first day of the Enrollment Term as set forth on the Enrollment Confirmation from Prime Subscriber.

d. Business Income Event means a Security Breach of Participant's Environment which actually and materially effects the Participant's business operations, resulting in actual, documentable loss of business income (net profit or loss before income taxes) which would have been earned had no Security Breach occurred.

e. Compliance Event means a BEC Event or Ransomware Event that involves a confirmed data breach of Personal Data triggering HIPAA, GDPR, UK GDPR, PCI, OSHA, SEC, FTC, and/or any international, federal, state or other legally required notice and/or reporting requirements, where the sole Recovery Benefit is for immediate legal assessment and emergency response of the Compliance Event. Continuing legal services beyond initial breach assessment, including dealing with the nature of the data breach and any extent of the same, are beyond scope of any Recovery Benefit of this Certification Warranty.

f. Cyber Legal Liability Event means litigation arising directly out of a breach of data privacy and/or data security because of a BEC Event or Ransomware Event and out of binding statements of privacy and/or security on Participant's website where legal defense expenses and settlement costs are incurred.

g. Enrollment Confirmation means the email issued by Prime Subscriber to Participant confirming Participant's enrollment in the Certification Warranty with Provider, which occurs upon Participant's enrollment via the Enrollment Portal.

h. Enrollment Term means the period Participant may receive a Recovery Benefit and which begins on the Benefit Start Date (defined in Section 2(a) and ends upon termination (defined in Section 10). Depending on the Benefit Start Date, generally the Enrollment Term is equivalent to the annual Subscription Term under the Solutions Agreement with the Prime Subscriber, for qualifying Subscriptions. In the case of a multi-year qualifying Subscription, an Enrollment Term under this Agreement will be those annual periods within a multi-year Subscription Term.

i. Environment means computer systems or networks identified by Participant and for which Prime Subscriber has implemented Solutions. Note any computer systems, networks, software or other tools of a dependent system, or any computer systems, networks, software or other tools not identified by a Participant to their Prime Subscriber as part of the Participant's Environment will not qualify for a Recovery Benefit, as such systems, etc., are not protected by Prime Subscriber Solutions. To be clear, this Warranty does not cover systems or environments Solutions are not purchased to secure.

j. Event means a Ransomware Event or BEC Event occurring in Participant's Environment, which may result in a Business Income Event, Compliance Event and Cyber Legal Liability Event.

k. Participant means the Customer who has contracted with Prime Subscriber to provide Solutions which protect the Environment that Participant has adequately and properly identified to the Prime Subscriber.

l. Prime Subscriber means Bitdefender and its Affiliates.

m. Personal Data means any information concerning an individual that is defined as personal information or personal data under any applicable data protection law; Personal Data does not include information lawfully available to the general public or that has been fully anonymized under an accepted industry standard.

n. Provider means Cysurance, a third-party service provider who has contracted with Prime Subscriber to provide Participant with the benefits set out in this Agreement.

o. Qualifying Event means a Ransomware Event or a BEC Event, or the Business Income Event, Compliance Event or Cyber Legal Liability Event resulting from a Ransomware Event or BEC Event occurring in Participant's Environment, for which Provider will apply a Recovery Benefit.

p. Ransomware Event means the unauthorized access to at least one Participant endpoint in Participant's Environment in the form of ransomware which has caused material harm to Participant, whereby “material harm” must include at least one of the following: (i) the unauthorized acquisition of unencrypted digital data from Participant's Environment that compromises the security, confidentiality, or integrity of personal information or confidential information maintained by Participant; (ii) public disclosure of personal information or confidential information from Participant's Environment and maintained by Participant; or (iii) the compromise of at least one Participant endpoint in Participant's Environment resulting in the full blocking of authorized access to such endpoint.

q. Recovery Benefit means the funding conferred to the Participant by the Provider in the event of a Qualifying Event; a Recovery Benefit is limited to supporting repair, remediation, and/or replacement of those parts of Participant’s Environment damaged by a Qualifying Event, including, but not limited to, removing and remediating elements that caused the Qualifying Event. A Recovery Benefit applies to immediate recovery services such as initial investigation to determine required services and restoration of Participant's current business systems covered by the Solutions. Continuing investigation concerning the extent of an actual or suspected Event, ongoing negotiations with a threat actor, procurement of new Solutions or recovery beyond Participant's Environment, legal evaluation of reporting obligations, or other ongoing breach services, are not eligible for a Recovery Benefit.

r. Security Breach means the (i) unauthorized access or use of Participant's Environment resulting from theft of a password from an agent of the Participant; (ii) a denial of service attack affecting Participant's Environment; or (iii) infection of a part of Participant's Environment by malicious code or the unauthorized transmission of malicious code from the Participant's Environment, which result in the loss of business income (net profit or loss before income taxes) which would have been earned had no loss occurred.

s. Prime Subscriber means the Bitdefender and its Affiliates engaged by the Participant to provide a Solution for the protection of Participant's Environment; such Solutions must be implemented and maintained by the Prime Subscriber for Participant in order for a Recovery Benefit to apply.

t. Solution or Solutions means the MDR Services which Participant has obtained, implemented and maintained provided by Prime Subscriber for the protection of Participant's Environment.

u. Enrollment Portal means the registration portal Participant must use to enroll and qualify for Certification Warranty benefits.

v. Waiting Period Not Applicable.

2. Certification Warranty

a. Benefit Start Date. Participant's Enrollment Term will begin on the Benefit Start Date.

b. Benefit End Date. Unless otherwise terminated earlier pursuant to Section 10 below, Participant's Enrollment Term will automatically terminate on the Benefit End Date.

3. Certification Warranty Benefits

a. During the Enrollment Term, Participant may submit a request for a Recovery Benefit by notifying Provider at bitdefender@cysurance.com/ or a form link: https://enroll.cysurance.com/bitdefender-claim-submission/, within at least the first forty-eight (48) hours of discovery of any actual Event, that one of the following Events has or may have occurred during the Enrollment Term:

· Ransomware Event;

· BEC Event;

· Compliance Event;

· Cyber Legal Liability Event; and/or

· Business Income Event.

b. Should an Event occur and be determined a Qualifying Event, and provided an exclusion set forth in Section 4 below does not apply, Provider will afford Participant a Recovery Benefit, subject to the following:

(1) Participant may only seek indemnification for one (1) Qualifying Event during the Enrollment Term;

(2) Participant must have a commercially reasonable basis and belief that damages resulting from the Event will exceed $5,000 USD or equivalent in applicable foreign currency;

(3) Recovery Benefit will not exceed Participant's maximum Certification Warranty Indemnification Level as specified within Participant's Enrollment Confirmation;

(4) Application of a Recovery Benefit in the form of cyber-insurance deductible-buy back, subject to the terms and conditions of Participant's cyber-insurance carrier, any terms and conditions of Provider, and to review and approval by both Provider and Participant's identified cyber-insurance carrier;

(5) Payment of any applicable deductible by Participant for the applicable Recovery Benefit; and

(6) Any Recovery Benefit is provided in accordance with any additional terms and conditions applicable to such Qualifying Event as specified in the Warranty Confirmation Summary attached hereto as **Schedule 1.**

c. Recovery Benefits are limited by this Certification Warranty. Participant is responsible for notice and coordination with any insurance carrier for any ascertain insurance claims. The provider is not an insurance carrier or coordinator.

4. Recovery Benefit Exclusions. A Recovery Benefit may be restricted to the country in which the Participant subscribed to the Solutions. A Recovery Benefit will not be afforded if any one or more of the following conditions occur regarding to the nature of the loss:

a. Participant fails to take commercially reasonable measures to: (i) undertake preventative maintenance, including but not limited to patching of any application and/or operating system running on an endpoint that is up to date per the timeframe for Common Vulnerability Scoring System (CVSS): Critical (score 8.5+) within 7 days, High (score 7-8.5) within 30 days; and Medium and Lower (score < 7.0) within 60 days, where each time frame is beginning from the date the fix is made available and if a reboot of the system or application was required in connection with any of the above, the application/system will not be considered to have fulfilled this requirement unless and until completion of the applicable reboot; and (ii) implement cloud or other back up measures of Participant's data to allow for recovery from a Ransom Event;

b. Participant fails to deploy multifactor authentication (MFA) on email, servers housing proprietary and privacy data, and operating systems essential business operations;

c. Participant fails to deploy industry standard and up-to-date anti-virus or comparable prevention tools on its endpoints;

d. Participant does not have the Solutions actively deployed in the part of the Participant's network or computer systems in which the Event occurred, such that there was no active deployment providing Prime Subscriber with means of receiving supported security relevant telemetry from such network or computer systems (i.e., infrastructure or endpoint);

e. Participant is in breach of Prime Subscriber's Contract or the Contract with Prime Subscriber has terminated or expired;

f. Participant is unable to provide proof of the Event or cannot verify the Event through log/event data;

g. The Breach Incident is occurring within a virtual desktop infrastructure (e.g. Citrix, VMware, and other virtual desktop infrastructure environments). For avoidance of doubt, this relates to both the device and operating system running the VDI management system/hypervisor and the virtualized operating system(s) running within each virtual instance;

h. The Breach Incident is caused by a third-party product and/or service which directly or indirectly causes the malfunction or nonperformance of the Product or the Subscription;

i. Situations where (i) the data is retrievable (i.e., Participant can get access to back-up data and is capable of restoring the majority of the deleted or encrypted data with the back-up); or (ii) where the data was not on the Bitdefender managed endpoints affected by the Breach Incident;

j. The Breach Incident is caused by a systemic failure of software impacting customers on a significant, large-scale basis;

k. The Breach Incident is caused by a systemic failure affecting the Bitdefender infrastructure;

l. Any Breach Incident that arises out of or is caused by, directly or indirectly, acts of God, including but not limited to earthquakes, hurricanes, tsunamis, natural disasters, wildfires, solar flares, solar winds, etc., acts of war or terrorism, or reasonably believed to be related to state sponsored cyberattacks, civil or military disturbances, nuclear, and interruptions, loss or malfunctions of utilities, communications, or the systemic failures of the same;

m. The Breach Incident arising directly or indirectly from the intentional or willful misconduct, collusion, or the negligence of the Customer, its Affiliates, or its or their directors, officers, agents, employees, non-employee workers, agents, representatives, contractors or consultants ("Customer Representatives");

n. The Breach Incident arising as a result of an infection, compromise, malware, virus or other unauthorized access of asset(s) or credentials that attempts to circumvent controls in an effort to compromise an endpoint that was introduced to Customer's internal systems (which could be an unprotected endpoint within the Customer network or a managed Bitdefender endpoint) by a Customer Representative, whether intentionally or unintentionally (e.g. malware or virus testing);

o. Customer is not in good faith or is considered non-meritorious or frivolous, as reasonably determined by Prime Subscriber;

p. After notification or an alert of a possible Event to Participant from Prime Subscriber, Participant fails to take reasonable measures or actions to investigate and adequately address any issues prompting such an alert from Prime Subscriber;

q. If a Participant is regulated by HIPAA, PCI, SEC, FTC, GDPR and/or any other international, federal, state or other law, regulation or rule:

i. Participant has not completed annual security and data risk assessments, or other necessary risk assessments, and documented risks;

ii. Protected Health Information ("PHI") or other protected information data inventory has not been fully completed and accounted for prior to an incident and claim;

iii. Subject to Participant's standard historical employment practices related to HIPAA, GLBA, CCPA, GDPR, UK GDPR or other data protection required training for employees, all of Participant's employees have not completed the necessary training within the 12 months prior to any incident and request for a Recovery Benefit;

iv. Participant has not adopted and adhered to applicable privacy and security policies, public facing, internal or otherwise, related to any international, federal, state or other legal or regulatory requirements to which Participant is subject prior to any Event;

v. Participant is named as a defendant, respondent, co-defendant or other defending party in a class-action lawsuit regarding the privacy requirement breach resulting from violation of any international, federal, state or other law, regulation or rule arising from or relating to an Event.

r. The Event did not occur during the Enrollment Term;

s. Participant does not submit the request for a Recovery Benefit for the Event during the Enrollment Term; or

t. Participant has not conducted an assessment or analysis regarding, or taken steps to assess its risks under, and adopted and adhered to, all applicable privacy and security laws, regulations and rules governing its processing of Personal Data prior to any Event.

5. Indemnification Process.

a. PARTICIPANT MUST IMMEDIATELY REPORT AN EVENT TO THE PROVIDER. FAILURE TO REPORT AN EVENT WITHIN FORTY-EIGHT (48) HOURS OF DISCOVERY WILL EXCLUDE SUCH AN EVENT FROM CONSIDERATION FOR A RECOVERY BENEFIT. WITHIN FIFTEEN (15) DAYS OF DISCOVERY OF ANY ACTUAL OR REASONABLY SUSPECTED EVENT, PARTICIPANT MUST SUPPLY PROVIDER WITH SUFFICIENT INFORMATION AS TO ALLOW PROVIDER TO VALIDATE DAMAGES INCURRED AND APPROPRIATELY EVALUATE THE NATURE AND CIRCUMASTNCES REGARDING THE ASSERTED EVENT OR THE REQUEST FOR RECOVERY BENEFITS WILL BE CLOSED IN THE EVENT OF INSUFFICIENT VERIFICATION OF LACK OF RESPONSE AS STATED HEREIN. IF PARTICIPANT FAILS TO DELIVER THE REQUESTED INFORMATION TO PROVIDER AS SET FORTH HEREIN, PARTICIPANT'S PROFFERED EVENT WILL BE TREATED AS AN INVALID EVENT THAT IS INELIGIBLE FOR A RECOVERY BENEFIT PURSUANT TO THE TERMS OF THIS AGREEMENT. AFTER THE INITIAL FIFTEEN (15) DAYS AND PARTICIPANT'S ORIGINAL PROVISION OF INFORMATION TO PROVIDER, ANY MAINTAINED FAILURE BY PARTICIPANT TO RESPOND OR PROVIDE EVIDENCE SUPPORTING RECOVERY BENEFITS FOR MORE THAN THIRTY DAYS WILL RESULT IN THE REQUEST FOR RECOVERY BENEFITS BEING CLOSED FOR LACK OF RESPONSE. ANY

DETERMINATION AS TO WHETHER AN EVENT IS A QUALIFYING EVENT, OR AS TO THE GRANT OF A RECOVERY BENEFIT, WILL BE MADE IN ACCORDANCE WITH THIS AGREEMENT.

b. Participant understands this Certification Warranty is separate and apart from, not affiliated with, and not issued by or part of any insurance product it has purchased, engaged or otherwise obtained. Participant is solely responsible for reporting any Event or Events to its insurance carrier regardless of whether Participant elects to request application of Recovery Benefits from Provider.

c. By submitting a request for a Recovery Benefit and submitting information to Provider, Participant understands and acknowledges Provider has separate terms and conditions related to privacy and data protection as set out on Provider's website terms, privacy policies, or other agreements made by and between Participant and Provider which will govern the use and protection of the information. Prime Subscriber does not accept liability or responsibility for Provider. Participant understands and agrees it is responsible for reviewing Provider terms, policies and agreements prior to submission of information. In the event Participant requests that Prime Subscriber provide information directly to Provider on Participant's behalf, Participant authorizes and consents to Prime Subscriber sharing the information with Provider, subject to the terms set forth in Sections 5(b) and 5(c) of the Agreement.

d. Indemnification made under the Certification Warranty is subject to the Provider's standards of review. If Provider denies indemnification to the Participant, notwithstanding anything to the contrary in this Agreement, Prime Subscriber shall have no liability to Participant.

e. To receive Recovery Services under the Service Warranty, Participant agrees to:

i. Provide documentation evidencing the Participant's date of enrollment in the Service Warranty;

ii. Provide log files and information about the symptoms and causes of a network compromise pertaining to the request for a Recovery Benefit, and all other information, documentation or things requested by Provider to assess the Event and any application of Benefits; and

iii. Verify cyber event via log files and/or other documentation or things concerning malicious code that resulted in any alleged loss of data and/or records triggering a violation of state and/or federal regulatory enforcement to which Participant is subject.

6. Additional Services

Following Participant's enrollment in the Service Warranty, and as part of the value conferred by the Service Warranty, Provider will perform, or have performed, regular scans of Participant's Environment from external sources. Results will be provided to Prime Subscriber to augment external monitoring and risk rating analyses that Prime Subscriber delivers to Participant as part of the Solutions. Such results may identify vulnerabilities related, but not limited to, the following:

1. **a.** Network Security
2. **b.** DNS Health
3. **c.** Patching Cadence
4. **d.** IP Reputation
5. **e.** Application Security
1. **f.** Threat Intelligence
1. **g.** Social Intel & Industry Intel
2. **h.** Information Leak including Dark Web scanning for credentials
1. **i.** Cloud Score

An initial scan will be conducted upon Participant's enrollment in the Certification Warranty and monthly thereafter during Participant's Enrollment Term. By enrolling in the Service Warranty, Participant consents to the receipt of such additional services by the Provider.

7. Cancellation

a. Prime Subscriber's Cancellation Rights.

Prime Subscriber may cancel the Program at any time for any reason.

b. Cysurance's Cancellation Rights.

If Prime Subscriber has not otherwise made the appropriate payment by the due date or any applicable renewal date, the Program may be cancelled for nonpayment in accordance with Section 11(b) of the Subscriber General Terms and Conditions Agreement and Program coverage will cease from the due date or renewal date.

Additionally, unless applicable local law provides otherwise, Cysurance may cancel this Program for Prime Subscriber's fraud or material misrepresentation upon sixty (60) days' prior written notice.

c. Effect of Cancellation.

See Section 11 of the Agreement for Effect of Cancellation.

8. Program Changes

Cysurance reserves the right to change the terms and conditions of the Certification Warranty Program at any time and will provide Prime Subscriber with sixty (60) days prior written notice of such changes. If any changes are made, such notice will be provided in a separate writing or email.

If Cysurance adopts any revision to the Program that would broaden Participant's coverage without additional cost or any increase in service fees and/or without changes to the terms and conditions applicable to the Program, the broadened coverage will immediately apply to the Program.

9. General Terms

(a) Cysurance may subcontract or assign performance of its obligations to third parties but shall not be relieved of its obligations to Prime Subscriber or any Participant in doing so.

(b) Cysurance is not responsible for any failures or delays in performing under the Program that are due to events outside of Cysurance's reasonable control.

(c) This Program may not be available in all jurisdictions and is not available where prohibited by law.

(d) In carrying out its obligations Cysurance may, solely for the purposes of monitoring the quality of Cysurance's response, record part or all the calls between Prime Subscriber and Cysurance.

(e) Cysurance represents and warrants that it has implemented commercially standard security measures, which will protect Confidential Information against unauthorized access or disclosure as well as unlawful destruction. Prime Subscriber or Participant will be responsible for the instructions it gives to Cysurance regarding the processing of its data, and Cysurance will seek to comply with those instructions as reasonably necessary for the performance of the Service and support obligations under the Program. Cysurance will be responsible for putting appropriate terms in place with any Participant related to the Confidential Information it receives from any Participant.

(f) Cysurance acknowledges and agrees to maintain compliance with the terms of the Data Protection Standards, GDPR and CCPA Privacy Addendum agreed upon with Prime Subscriber.

(g) There is no informal dispute settlement process available under this Program.

(h) As used in this Program, "Cysurance" is the Administrator.

(i) Except where prohibited by law, the laws of the State of New York govern Programs purchased in the United States. If these terms are inconsistent with the laws of any jurisdiction where Participant purchases this Program, including the laws of Alabama, Arizona, Florida, Georgia, Nevada, Oregon, Vermont, Washington, Wisconsin and Wyoming, then the laws of that jurisdiction will control.

(j) Support services under this Program may be available in English only.

Schedule 1 of Annex 1

Cysurance Certification Warranty Program Confirmation Summary

Subject to all of the terms and conditions of the Program, including any terms specified on Annex 1 to which this Schedule 1 is attached, the Program provides the following coverage limitations:

Participants Enrolled in the $100,000 Level		
Certification Warranty Indemnification – Ransom Only **$100,000 Level** Ransom Event	**Per Event** $100K*	**Per Participant** $100K* *Per Event and Per Participant amounts vary and are Program specific.

Indemnification Per Event and Per Participant amounts reflected above, although shown in USD, means the equivalent amount in the applicable foreign currency reflected on Participant's subscription for the Warrantied Software System.

* Participant must first exhaust any other Certification Warranty that would apply to these expenses.

**Cyber Legal Liability/Media - Participant must exhaust all other financial benefits before triggering this benefit tier.

EXHIBIT C – SPECIAL TERMS AND CONDITIONS FOR BITDEFENDER OFFENSIVE SECURITY AND CYBERSECURITY ADVISORY SERVICES

Bitdefender and Customer may enter in one or more Statements of Work (SOWs), which will be governed by the terms of this Master Service Agreement setting forth additional obligations between them.

2. PROVISION OF SERVICES

2.1. Scope and Content of Services

Bitdefender shall provide the Services to Customer in accordance with the terms and conditions of this Agreement and of the applicable SoW signed by Parties, having all the details established in the Technical Scoping Exhibit of the SOW. Apart from documentation, manuals, and software directly acquired in conjunction with and necessary for the Services provided, no other materials shall be supplied under this Agreement.

The precise scope of Services to be provided by Bitdefender shall be defined in a Statement of Work.

The Customer or any of its Affiliates may enter into Statements of Work with Bitdefender under this Agreement.

Bitdefender's ability to deliver the Services described in Statements of Work depends upon full and timely cooperation by Customer and Customer's staff, as well as the accuracy and completeness of any information provided. Bitdefender may provide Customer additional assumptions in writing in the respective Statements of Work before providing any Services thereunder.

Bitdefender may provide some or all the Services to Customer via the encrypted platform. Further to this provision of Services via the encrypted platform, Customer may receive Access Credentials from Bitdefender.

Upon Bitdefender' acceptance of Customer's order as stated in the SoW and in consideration of the payment of the fee by Customer and receipt of the corresponding payment by Bitdefender or its authorized resellers or distributors, Bitdefender shall provide the Bitdefender Offensive and Cybersecurity Advisory Services that Customer ordered according to the respective SOW, solely for Customer's internal business operations and subject to the terms of this Agreement. Customer may allow its Authorized Users to use Bitdefender Offensive and Cybersecurity Advisory Services for this purpose and Customer is responsible for their compliance with this Agreement with respect to such use.

Bitdefender will endeavor to confirm resources for the project as soon as a signed project confirmation sheet has been received, and the Technical Scoping has been agreed. The dates will only be confirmed once written acceptance for these dates has been received. Once dates have been accepted, Bitdefender will ensure that resources are assigned and thereafter the late cancellation policy will come into effect.

All Services shall be performed remotely by Bitdefender unless the Customer specifically requests for on-site performance by Bitdefender personnel and Bitdefender expressly agrees in writing with such Customer request. In the case of on-site performance of the Services, the expenses incurred by Bitdefender personnel shall be paid by the Customer according to article 3.3. below.

The description of the Services is included in the Appendix A below. Any other Services performed by Bitdefender to the Customer and described and agreed with Bitdefender in writing in the Technical Scoping and not expressly included in Appendix A below, shall also be governed by this Agreement. Please be advised that, depending on the particularities or nature of such services, specific Service Levels and/or prerequisites may apply in lieu of or in addition to those mentioned in this Agreement and shall be included in the Technical Scoping.

2.2. Service Level. Bitdefender will make the Services available to the Customer in accordance with Service Levels hereto. Bitdefender may update the Services during the Term, however, at no time will an update materially diminish the function of the Services.
Bitdefender shall provide the following Service Levels:

· for Penetration Test Services: i) Final Report for the assessment to be provided within 5 (five) business days after the scheduled reporting day, ii) Final Report for the assessment to be updated within 5 (five) business days after the scheduled retest day.

· for Red Team Services: Final Report for the assessment to be provided within seven business days upon completion of the assessment.

These SLAs presented above depend on the fulfillment of the prerequisites stated below.

2.3. Prerequisites: Before Bitdefender starts the delivery of the Services, meaning before the Start Date, Customer must obtain all necessary rights and permissions from all its Users and must fulfill the following:

2.3.1. Penetration Testing - Web Application Assessment prerequisites:

· Confirmation of in-scope URL;

· Provisioning of 2 sets of accounts for each User role;

· Each User account to be provisioned with sample test data;

· No infrastructure or code changes to be made during the assessment period;

· Whitelisting of Bitdefender's external testing IP addresses, 13.76.47.44, 52.230.87.131 and 34.87.70.149 (for external assessments);

· Whitelisting of Bitdefender's testing IP addresses from any WAF, IPS, or IDS systems;

· If the case for online assessment, logistics for onsite assessment to be provided during the time of testing (including tables, chairs, electricity, network connectivity, on-demand physical access, relevant authorization and permissions, etc);

· Temporary disable 2FA and CAPTCHA validation (if any) and enable it upon request;

· Technical point of contact for any queries during the assessment;

· Consultants' mobile numbers to be tied to SMS 2FA mechanism (where applicable).

2.3.2. Penetration Testing – Web API Assessment prerequisites:

· Provisioning of full API project Postman/Swagger files;

· Full API documentation, with details on functions, parameters, and expected responses;

· Sample API request data for all in-scope API calls;

· Provisioning of 2 sets of credentials for each User role (where applicable);

· Each User account to be provisioned with sample test data;

· Provisioning of means to generate API authorization keys/tokens (where applicable);

· No infrastructure or code changes to be made during the assessment period;

· Whitelisting of Bitdefender's external testing IP addresses, 13.76.47.44, 52.230.87.131 and 34.87.70.149 (for external assessments);

· Whitelisting of Bitdefender's testing IP addresses from any WAF, IPS, or IDS systems;

· If the case, Logistics for onsite assessment to be provided during the time of testing (including tables, chairs, electricity, network connectivity, on-demand physical access, relevant authorization and permissions, etc.);

· Temporarily disable 2FA and CAPTCHA validation and enable it upon request;

· Technical point of contact for any queries during the assessment.

2.3.3. Penetration Testing-External/Internal Network Assessment prerequisites:

· Confirmation of in-scope IP addresses;

· Provision of authentication credentials to log into the in-scope devices (For Grey-box only);

· Whitelisting of Bitdefender's testing IPs on port 135,445 for Windows devices or port 22 SSH for Unix-based devices (For Grey-box only);

· No infrastructure changes to be made during the assessment period;

· Whitelisting of Bitdefender's external testing IP addresses, 13.76.47.44, 52.230.87.131 and 34.87.70.149 (for external assessments);

· Whitelisting of Bitdefender's testing IP addresses from any WAF, IPS, or IDS systems;

· Technical point of contact for any queries during the assessment.

2.3.4. Penetration Testing- Mobile Application Assessment prerequisites:

· Provisioning of 2 sets of accounts for each User role;

· Each User account to be provisioned with sample test data;

· Provisioning of Android APK and iOS IPA binaries, without security mechanisms in place, if present (root/jailbreak detection, SSL pinning, anti-debugging, etc.);

· Provisioning of Android APK and iOS IPA binaries, with security mechanisms in place, if present (root/jailbreak detection, SSL pinning, anti-debugging, etc.);

· No infrastructure or code changes to be made during the assessment period;

· Whitelisting of Bitdefender's external testing IP addresses, 13.76.47.44, 52.230.87.131 and 34.87.70.149 (for external assessments);

· Bitdefender's testing IP addresses to be whitelisted from any WAF, IPS, or IDS systems;

· Technical point of contact for any queries during the assessment.

2.3.5. Red Team (Adversarial Attack Simulation Exercise) Assessment prerequisites:

· Confirm the Red Team (Adversarial Attack Simulation Exercise) objectives.

· Customer to assign technical point of contact to:

1. Provide logistics and other information required, prior to commencement of the engagement.

2. Respond to any technical queries during the assessment.

3. Confirm out-of-scope elements e.g specific system or critical servers, specific departments or individuals for social engineering, phishing or any other attacks.

4. Provide a seeded access laptop for the Assume Breach phase and support to execute the payload, if required.

· As Bitdefender performs actions across the cyber kill chain, seeded access or information may be required to increase the efficacy of the engagement. It is advisable that Customer prepares the following information and resources to be provided to Bitdefender when it is necessary, including but not limited to:

1. Additional information such as network diagram, onboarding information as if a new employee, list of technologies used such as EDR, email security, SIEM, NAC, etc.

2. One or more standard built laptops, with domain-joined User accounts of varying privileges that are based on department or roles.

3. Access to the network via VPN or a jump host.

4. The red team consultant mobile numbers to be tied to SMS 2FA mechanism for VPN, cloud applications, etc., if required.

· Letter of authorization from board of director / project sponsor and point of contact for potential escalations during physical assessment.

· Bitdefender and Customer to implement proper risk management strategy.

In case Red Team Service is delivered using a gated approach, Bitdefender may not be able to resume the Red Team exercise immediately upon request. The request will be served on the next earliest available time slot of the Red Team consultant. Bitdefender will maintain the Command and Control (C2) and phishing infrastructure for a maximum of two (2) months between stages. Thereafter, should the next stage not have been initiated, the project will be deemed to have been concluded.

2.3.6. Cybersecurity Advisory Services main prerequisites:

· Customer must provide Bitdefender with a main point of contact, with access to relevant stakeholders and documentation if required by the service.

2.4. Services Restrictions. Customer shall use the Services according to the agreed use cases and as agreed in the Technical Scoping Exhibit.

Customer shall neither directly nor indirectly: (i) interfere with or disrupt the integrity or performance of the Services or the data contained therein; (ii) attempt to gain unauthorized access to the Services or their related systems or networks; (iii) use the Services, or permit them to be used, for purposes of product benchmarking, competitive research, or other comparative analysis without Bitdefender's prior written consent; (iv) use the Services for a use other than as set forth in the Technical Scoping.

The Services are protected by know-how laws and international copyright treaties, as well as by other intellectual property laws and treaties. This Agreement only gives Customer some rights to use the Services.

The precise scope of the Services to be provided shall be as described in the Technical Scoping Exhibit only, and Bitdefender shall not be required to provide any other Services other than those expressly agreed. All changes to the scope must be agreed upon in writing by both parties. In the event the number of findings require more Retest days than what was initially scoped, a separate SOW will be raised and invoiced for the additional days required. Assessment activities conducted within localized out-of-office hours (18:00 – 09:00), or (09:00-18:00) weekends or public holidays will be charged at 1.5 x standard day rate. Weekends or public holidays combined with unsocial hours (18:00-09:00) will be charged at 2.0 x standard day rate.

2.5. Access and License to Customer Data. Customer grants Bitdefender a non-exclusive, worldwide, royalty-free, fully paid-up right and license to copy, access, transmit and otherwise process the Technical Data to provide the Services to Customer as set forth in this Agreement. Bitdefender will not access Customer Data except (i) to provide the Services and the associated support services; (ii) to prevent or address service, security or technical problems with the Services; (iii) to audit Customer's use of the Services and to confirm Customer's compliance with the Agreement; (iv) to aggregate de-identified information regarding Customer's usage and configuration metrics of Services (which in no event shall include Customer Data) with that of other Bitdefender customers and use such aggregated customer services data as part of the Services; (v) as compelled by law; or (vi) as Customer expressly permits in writing.

2.6. Customer Responsibilities. Customer is responsible for the acts and omissions of all Users in connection with this Agreement, as well as any and all access to and use of the Service by any User or any other person logging in under a User ID registered under Customer's account, even if a claim may not be enforceable directly against those Users, due to lack of power or authority, discharge, offset or defense. The Customer is responsible for the networking and hardware data security for the Services to the extent the Services are deployed on Customer-controlled networks or hardware, including the legal and operational consequences of its configuration. Customer acknowledges that Customer's access information, will be Customer's "key" to the Services; accordingly, Customer will be responsible for maintaining the confidentiality of such access information. Customer will: (i) notify Bitdefender promptly of any unauthorized use of any password or account or any other known or suspected breach of security; (ii) not impersonate another Bitdefender user or provide false identity information to gain access to or use the Services.

Bitdefender may use its own independent contractors to perform the Services, in which case Bitdefender will be responsible for the performance of such independent contractors.

Bitdefender hosts portions of the Services either directly or subcontracted through a third-party hosting provider; and some configurations of the Services may require Customer cooperation on Customer controlled hardware. Subject to the terms and limitations on relevant SoW, Bitdefender grants to Customer during the Term the worldwide, non-exclusive, revocable, limited, non-transferable, royalty-free right for the Authorized Users to access and use the Services and Documentation consistent with the Documentation and the SoW solely for its internal business purposes or as otherwise indicated in the applicable SoW.

2.7. Acceptance. The parties shall agree upon the acceptance criteria. Customer shall send a notice to Bitdefender if failure to confirm with the acceptance criteria within 7 (seven) days from completion of the Services. The Services are deemed to be accepted in 2 (two) weeks following completion of the Services or if the Customer has made the payment. The respective Services or partial Services are furthermore always deemed accepted if the Services are used for productive purposes.

3. PAYMENT TERMS

3.1. Service Fees. Customer will pay Bitdefender the Services fees and any other amounts for Bitdefender's Services ordered by Customer as stated in the SOW and agreed within the Technical Scoping of the Services, either directly or through the Bitdefender channel partner contracted (collectively, the "Service Fees").

Unless otherwise agreed with the channel partner, all Service Fees will be invoiced in advance in accordance with the purchase order submitted to the channel partner. Unless otherwise set forth in the purchase orders, all Service Fees are due and payable Net 30 days after the date of the applicable invoice. All invoices that are not paid within 30 days, and all credit accounts that are delinquent shall be assessed a 1% late payment charge (or if this exceeds the legally permitted maximum, the highest legal rate under applicable law) for each month the invoice is not paid, or the account is delinquent. Customer will reimburse Bitdefender or its resellers for all reasonable costs (including reasonable attorneys' fees) incurred by Bitdefender or its resellers in connection with collecting any overdue amounts. Except as otherwise specified in this Agreement, the payment obligations are non-cancelable and the Service Fees paid are non-refundable, and the purchased Services cannot be decreased or exchanged for alternative Services or subscriptions.

3.2. Taxes. All Service Fees are exclusive of all sales and use taxes, value-added taxes, excise taxes, levies, or duties which may be imposed by applicable national or federal, state/provincial or local municipalities relating to Customer's purchase of subscriptions or use of the Services (the "Taxes"), and Customer will be responsible for payment of all such Taxes. Unless Customer provides Bitdefender or its resellers with evidence of its sales tax exemption, Customer shall pay Bitdefender all relevant taxes payable related to Customer's purchases, excluding taxes based on Bitdefender's net income. Customer will pay all Service Fees free and clear of, and without reduction for, any such Taxes, including withholding taxes imposed by any country. Customer will provide receipts issued by the appropriate taxing authority to establish that such Taxes have been paid.

3.3. Expenses. The Customer shall pay Bitdefender for all reasonable travel, out-of-pocket and living expenses (if any) incurred by Bitdefender personnel in connection with the on-site performance of the Services if such performance was requested by the Customer and was prior agreed in writing by Bitdefender.

3.4. Cancellation. If all or part of the Services is to be canceled or postponed once booked and confirmed, Bitdefender requires at least 10 days prior notice. If Service is to be canceled/postponed less than 10 days prior to the agreed start date, the following charges will be incurred:

Timing of notification of cancellation or postponement	Fee payable
>11 business days before the agreed Delivery Start Date	**No cancellation fee**
Between 6 and 10 days before the agreed Start Delivery Date	**50% of the project fee**
<5 days before the agreed Start Delivery Date	**100% of the project fee**

3.5. Report. Provided that Customer has fully paid all applicable Service Fees in relation to the relevant Report, Bitdefender hereby grants Customer a license to use all such rights on a non-exclusive, non-sublicensable, non-transferable, worldwide, royalty-free and perpetual basis to the extent necessary to enable Customer to internally use the Report, as described in the applicable Statement of Work.

Customer shall not: (i) rent, lease, modify the Report without the prior written consent of Bitdefender; ii) transfer licenses to, or sublicense, fixes and/or to the Report to any third party including the national governments.

Appendix A to Exhibit C

Description of Offensive Security Services and Cybersecurity Advisory Services

A.1. BITDEFENDER OFFENSIVE SECURITY SERVICES:

Penetration Testing- Web Application:

Bitdefender will perform a time limited web application penetration test against the application(s).

Penetration Testing – Web API:

Bitdefender will perform a time limited web API penetration test against the web APIs.

Penetration Testing-External/Internal Network:

Bitdefender will perform a network security assessment against the in-scope IP addresses.

Penetration Testing- Mobile Application:

Bitdefender will perform a mobile application security assessment against the application(s) Android and iOS operating systems.

Red Team (Adversarial Attack Simulation Exercise):

Bitdefender will perform red team attack simulation service, which is a threat-focused, objective-based assessment with the goal of stress-testing the detection and response capabilities from simulated real-life, advanced, and targeted threats.

This will be delivered using a phased approach. The following is a high-level overview of the sequence of events:

1. **Project Initiation Phase** (Pre-Commencement): Confirmation of engagement objectives, project working group, risk management framework, and project cadence.
2. **Initial Access Phase** (Start of the Engagement): Bitdefender utilizes the pre-planned scenarios (i.e., email phishing) in an attempt to obtain initial access into the client network.
3. **Breach/Assume Breach Phase: i.** Access into client network is seeded/provided by client if Initial Access attempts were unsuccessful; **ii.** Utilizing access achieved/provided, Bitdefender will attempt to achieve pre-agreed objectives to demonstrate impact to the client.
4. **Attack Disclosure Phase: i.** Within the last week of the **Breach/Assume Breach Phase**, if Bitdefender remains undetected, the client's security/response team will be notified; ii. Metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) can be measured at this phase.
5. **Reporting Phase:** Bitdefender will document, quality assure and finalize the engagement report which will detail all findings and recommendations.
6. **Management Presentation** (End of Engagement): Bitdefender will conduct a formal presentation of findings to the client's management/technology stakeholders.

If a request has been made for this to be delivered using a gated approach, each phase of the red team engagement will only commence upon receiving an email approval*. This will be after the **Initial Access Phase** completion and Bitdefender Red Team will resume either the **Assume Breach** or **Breach Phase** depending on the outcome of Initial Access phase. These will be defined in the Technical Scoping Exhibit.

Host Configuration Review

Bitdefender will perform a configuration review against the in-scope hosts.

The total number of host(s) in scope shall be included in the Technical Scoping.

Phishing Simulation

Bitdefender will perform a simulated phishing attack against the chosen organization.

Cloud Security Assessment

Bitdefender will perform Cloud Security Assessment against the in-scope Cloud infrastructure.

The total number of cloud accounts in scope shall be included in the Technical Scoping.

Smart Contract Audit

Vendor will perform a Smart Contract audit service on a specific number of lines of code that will be included in the Technical Scoping.

A.2. CYBERSECURITY ADVISORY SERVICES:

Cybersecurity Advisory Retainer:

Cybersecurity Advisory Retainer is a flexible, scalable and retainer-based solution allowing organizations undergoing digital transformation to build security and compliance capabilities using our experienced cyber strategists in a flexible way.

Cyber Security Review:

An assessment that reviews an organization against a holistic and industry recognized cyber security framework such as ISO27001, NIST CSF or CIS. Understanding how cyber security is managed across Customer organization is critical to understanding where to prioritize investment and resources to ultimately reduce risk.

Cyber Security Strategy:

Definition or review of an organization's Cyber Security Strategy to help drive the direction of Cyber Security risk management.

Training and Awareness:

Bitdefender tailored training and awareness programs equip board members and employees with the knowledge and skills to manage, recognize, prevent, and respond to cybersecurity risks through better awareness and understanding. Through topic specific training or broader cyber security awareness, we cultivate a culture of heightened awareness, reducing the likelihood of human error.

Reporting and Dashboarding:

Cyber security is another business risk and managing it effectively is critical to operating a business. The ability to showcase a positive ROI is often hard given silence is positive. We are able to support the definition of or review organizations existing KPIs, metrics or wider reporting and dashboarding capability to report on the ROI of security investment.

Risk Assessment:

Cyber security is another business risk and managing it effectively is critical to operating a business. An assessment of an organization's risk profile (by identifying the top threats and vulnerabilities facing Customer organization), or the risk associated with a specific project, application or asset using industry recognized methodologies such as IRAM2, NIST RMF, ISO27005.

Compliance Support:

Compliance services against well-known industry standards such as ISO27001 or PDPA, to support Customer organization identify gaps in compliance and provide recommendations or support with accreditation. Our report will document all non-conformities or non-compliance with the chosen standard or framework.

Supply Chain/Third Party Risk Management:

Defining and implementing a third-party risk management framework to consistently manage third parties. This would include the option for organizations to outsource the management of third parties to Bitdefender to perform. Organizations can tailor the service to include only critical and high suppliers or however they need to supplement their existing team capabilities.

Information Security Policy Framework Development:

Our team will collaboratively craft comprehensive policies tailored to Customer specific needs, ensuring alignment with relevant industry standards and compliance mandates. Through meticulous procedure development, we establish clear guidelines for the management of cyber security risk bolstering Customer resilience against cyber threats.

Incident Response Tabletop Exercises:

A simulated scenario designed to evaluate Customer organization's readiness against potential cyber threats. Participants will navigate through a number of hypothetical security breaches with our team of experts, testing their decision-making, communication, and collaboration skills. This hands-on exercise provides a risk-free environment to identify gaps in Customer response strategy, refine procedures, and enhance overall cybersecurity resilience.

Project Management for Security Transformation:

Provide project management support for large complex transformation programs with multiple workstreams operating concurrently.

EXHIBIT D – SPECIAL TERMS AND CONDITIONS FOR BITDEFENDER THREAT INTELLIGENCE SOLUTIONS

Bitdefender and Customer may enter into one or more purchase orders for Bitdefender Threat Intelligence Solutions and the associated Threat Intelligence Data, which will be governed by the terms of this Master Service Agreement, setting forth additional obligations between for use of the Bitdefender Threat Intelligence Solutions and the associated Threat Intelligence Data, as well as Sandbox Malware Analysis and any other associated services provided by Bitdefender, hereinafter.

1. RIGHTS GRANTED AND RESTRICTIONS

1.1. For Internal Use Rights. If stated in the Commercial Documentation and upon Bitdefender's acceptance of order and in consideration of the payment fees made by Client and the successful receipt of the corresponding payment by Bitdefender or its authorized channel resellers or distributors, Bitdefender grants to Client a limited, non-exclusive, non-transferable, non-sublicensable access and use right of Bitdefender Threat Intelligence Solutions, solely on Client behalf and Client's benefit without the right to market, distribute, resell or exhibit outside Client organization. For clarification purposes, internal use does not include access or use: (i) for the benefit of any person or entity other than Client or (ii) in any event, for the development of any kind of product or service. The access and usage right is limited to the quantities specified in the Commercial Documentation in accordance with any applicable Documentation during the applicable Validity Period.

1.2. For Providing Services Use. If stated in the Purchased Order signed with Bitdefender, and upon Bitdefender's acceptance of order and in consideration of the payment fees made by Customer and the successful receipt of the corresponding payment by Bitdefender, Bitdefender

grants Customer the limited, non-exclusive, non-transferable non-sublicensable right to access and use Bitdefender Threat Intelligence Solutions solely for providing security managed services as specified in Purchase Order as Customer Service to the Users of the Customers which are allowed to use it for their Internal Use based on an agreement with Customer. The Service Providing Use is limited to the applicable Validity Period and only in accordance with any applicable Documentation.
For clarification purposes, Providing Services Use does not include access or use: (i) for the benefit of any person or entity other than Users of the Customer or (ii) in any event, for the development of any king of product or service other than Customer Service stated in the Purchase Order. The access and usage are limited to the quantities specified in the Commercial Documentation in accordance with any applicable Documentation during the applicable Validity Period.

1.3. Limitations of rights granted.

1.3.1. Fair Usage conditions.

For this purpose, Customer may allow Users to use Bitdefender Threat Intelligence Solutions and Customer is responsible for their compliance with these Terms in such use where applicable as per the rights granted to the Client within the Purchase Order signed with Bitdefender.

Customer shall use Bitdefender Threat Intelligence Solutions according to the agreed use cases and agrees not exceed the usage limits as specified in the Documentation and herein.

Customer is not allowed to:

(a) overload Bitdefender Threat Intelligence Solutions beyond the normal usage;
(b) perform any kind of stress testing on Bitdefender Threat Intelligence Solutions;
(c) conduct any kind of penetration testing on Bitdefender Threat Intelligence Solutions such as port scanning, vulnerability scanning, traffic replay or others;
(d) use Bitdefender Threat Intelligence Solutions data during penetration testing outside Customer premises, without prior written approval of Bitdefender;
(e) attempt to access Bitdefender Threat Intelligence Solutions which requires authorization, with missing or modified authorization tokens;
(f) make any changes or alter anyhow the data received from Bitdefender Threat Intelligence Solutions;
Bitdefender Threat Intelligence Solutions products and services are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Bitdefender Threat Intelligence Solutions are not licensed, nor sold. These Terms only give Customer specific rights to use the Bitdefender Threat Intelligence Solutions for Internal Use unless specifically agreed in writing within a Purchase Order signed with Bitdefender.

1.3.2. Usage Restrictions

(a) Under the Agreement, Customer may not transfer or sublicense Bitdefender Threat Intelligence Solutions to another person or legal entity, Customer shall not rent, lease, loan, auction, or resell Bitdefender Threat Intelligence Solutions nor modify, translate, or create derivative works, reverse engineer, de-compile, or disassemble Bitdefender Threat Intelligence Solutions, in whole or in part, or otherwise attempt to reconstruct or discover the source or object code or underlying ideas, algorithms, file formats, programming or interoperability interfaces (or if the law permits any such action, Customer agrees to provide at least ninety (90) days written notice in advance);

(b) Customer may not permit third parties to benefit from the use or functionality of Bitdefender Threat Intelligence Solutions via a timesharing, service bureau or other arrangement or as part of any other hosted or platform service that permits either access to or use of Bitdefender Threat Intelligence Solutions, whether on a specific fee basis or otherwise.

(c) This Agreement only gives Customer specific rights to use Bitdefender Threat Intelligence Solutions for Internal Use unless specifically agreed in written within a Purchase Order signed with Bitdefender.

(d) Customer may not remove any proprietary notices or labels on Bitdefender Threat Intelligence Solutions and Customer may not disclose results of any program benchmark tests without Bitdefender's prior written consent.

(e) Additionally, Client may not, (a) modify, block, circumvent or otherwise interfere with any authentication, license key or security measures in the Bitdefender Threat Intelligence Solutions, (b) distribute, license, sublicense, lease, sell, rent, loan, mortgage, encumber, auction, or otherwise transfer or provide a copy of any Bitdefender Threat Intelligence Solutions (or components thereof including any license or access key or authorization to any third party; (c) publish, provide, or otherwise make available to any third party, any competitive, performance, or benchmark tests or analysis relating to the Bitdefender Threat Intelligence Solutions without the written permission of Bitdefender which may be withheld or conditioned at the sole discretion of Bitdefender; (d) deploy or use Bitdefender Threat Intelligence Solutions in any manner other than as expressly permitted in its Documentation; or (e) attempt to do any of the foregoing.

(f) Customer is responsible for obtaining all necessary rights and permissions from Users to use their data with Bitdefender Threat Intelligence Solutions.

Bitdefender Threat Intelligence Solutions products and services are designed and intended to be used in defensive security products and solutions. Any and all usage, including direct, indirect or associative usage of the intelligence provided for offensive security purposes (such as, but not limited to: penetration testing, red teaming, application security & reverse engineering) is not allowed, except for particular situations, previously and explicitly allowed in writing by Bitdefender.

Moreover, all use of Bitdefender Threat Intelligence Solutions, is not allowed to lead to (i) any disclosure of any entity name affected or compromised by cyberthreats; or (ii) unlawfully identifying and attacking the potential attackers which is strictly forbidden. Notwithstanding anything to the contrary herein, such disclaimer is allowed strictly and solely if said usage is explicitly stated as a valid and intended use-case within the contract scope or allowed by a legal authority.

1.3.3. Entitlements and limits of the usage rights

Unless otherwise agreed in the Commercial Documentation the following entitlements and limits shall apply:

Bitdefender IntelliZone Portal							
Company size (number of End Users)	up to 1000	up to 2000	up to 5000	up to 10000	up to 25000	up to 50000	up to 100000
Bitdefender IntelliZone Portal accounts included	3	3	5	8	10	15	20

Bitdefender TI Threats API calls included per year	100000
Sandbox Malware Analysis submissions per year	1000

Bitdefender Threat Intelligence Feeds	
Reputation Threat Intelligence Feeds	
Peak rate limit (requests per minute)	5 requests / minute
Operational Threat Intelligence Feeds	
Peak rate limit (requests per minute)	30 requests / minute

Bitdefender Threat Intelligence Threats API	
Peak rate limit (requests per second)	25 requests / second

Sandbox Malware Analysis						
Submissions per month	250	500	1000	2500	5000	1000
Submissions per day	20	30	50	100	250	450
Maximum file size (in MB)	50	100	100	100	100	100
Bitdefender IntelliZone Portal accounts included	3	3	5	8	10	15

2. UPDATES

2.1. Customer must comply with the payment obligations for Bitdefender Threat Intelligence Solutions or have an active subscription, as applicable, to receive Updates or Upgrades.

3. TERM OF USAGE

3.1. Customer will receive Bitdefender Threat Intelligence Solutions based on the subscription acquired and Customer will have certain rights to access and use Bitdefender Threat Intelligence Solutions during the Validity Period as stated in the Purchase Order, Customer which shall last for the period of time set forth in the Commercial Documentation or the applicable order to Bitdefender or its distributor or channel reseller from which Customer acquired Bitdefender Threat Intelligence Solutions. Bitdefender Threat Intelligence Solutions may be automatically deactivated at the end of the Validity Period and Customer will not be entitled to receive any feature or content updates to the Bitdefender Threat Intelligence Solutions.

Further, if Customer does not continue to abide by the terms of this Agreement, Customer acknowledges that doesn't have any right to use Bitdefender Threat Intelligence Solutions and agrees with the termination of the Agreement and will uninstall and not use Bitdefender Threat Intelligence Solutions forthwith.

3.2. Bitdefender reserves the right to stop supporting its products or a version of its products or to discontinue its Products or Product features, subject to the End-of-Support policy published on its websites.

4. TECHNICAL SUPPORT SERVICES

4.1. Technical support for Bitdefender Threat Intelligence Solutions is included in the fees for the Validity Period. Certain technical support features may be offered by Bitdefender through its channel resellers for the subscription term of Bitdefender Threat Intelligence Solutions as stated on Bitdefender's website and Commercial Documentation. Technical Support shall be governed by the following conditions: Any such Technical Support shall be provided without any guarantee or warranty of any kind.

4.2. Standard Support: The terms and conditions of standard technical support for Bitdefender Threat Intelligence Solutions are stated here: https://www.bitdefender.com/site/view/enterprise-support-policies.html.

Bitdefender reserves the right to refuse, suspend or terminate any of the Technical Support in its sole discretion in case Customer is in breach of obligations. The technical support policies are subject to change at Bitdefender's discretion. However, Bitdefender will not materially reduce the level of services provided for supported programs during the period for which fees for technical support have been paid. Customer should review the policies published on websites prior to entering the ordering document for the applicable services. If Customer intends to receive any professional services, then Customer needs to sign a separate statement of work with Bitdefender. These terms are not applicable for any Trial/Beta/Early Access etc. Solutions, for which Bitdefender does not offer any technical support service.