Trend Micro

General Service Description
Applicable to Service One

This General Service Description applies to each Service One Offering (as defined below) provided by Trend Micro and together with the applicable Specific Service Description form the entire Service Description applicable to the Service One Offering purchased by Company from Trend Micro. The Service Description forms a part of the Master Terms Of Service (as defined below) with respect to each Service One Offering provided thereunder.

1. Introduction – Service One; Overview; Additional Agreed Definitions.

1.1 Introduction – Service One; Overview.

1.1.1 Introduction – Service One. Trend Micro Service One ("**Service One**" herein and "Cloud Services" when referenced in the Master Terms of Service) are services that are made available by Trend Micro for additional compensation in connection with certain supported Trend Micro Technologies (as defined below) that are required in order for Trend Micro to perform and provide a purchased Service One Offering. The Service One Offering is an optional service that may be purchased by Company at any point in its deployment of Trend Micro Technologies that provide, if purchased, additional enhanced services and competency in connection with deployed Trend Micro Technologies as is more fully described herein

1.1.2 Overview. Each Service One Offering includes priority technical support assistance, proactive health checks, early warning of high-profile threat campaigns and priority scheduling for incident response services to allow Company to help prepare for, withstand, and rapidly recover from threats as set forth below.

1.2 Service One Offering Service Term. Each Service One Offering is provided for a Subscription Period of no less than one (1) year and no more than three (3) years as set forth in the applicable Certificate therefor, which Subscription Period is non-cancelable and the fees for each Service One Offering are non-refundable once Service One Offering is Ordered and accepted by Trend Micro. The period of performance of each Service One Offering will not be deferred even if Company has not deployed, installed, or configured the required Trend Micro Technologies.

1.3 Complete Agreement for Service One Offering. The sole and only agreement between the Parties for each Service One Offering is comprised of the following in descending order of precedence: (**a**) the Master Terms of Service in effect on the date that the Certificate is issued to Company in connection with the procurement of a Service One Offering; (**b**) this General Service Description applicable to the Service One Offering; and (**c**) the applicable Specific Service Description; *provided*, *however*, a lower tier document may modify the next higher tier document with respect to that lower tier document, by specifically referencing a provision in next higher tier document being modified or superseded, in which event such modification shall govern and control only for purposes of that lower tier document. **Because each Service One Offering is a fixed-scope Cloud Service that is offered by Trend Micro, the Parties understand and agree that no Service Description may be modified or amended by the Parties, and any attempt to do so will be void.**

1.4 Additional Agreed Definitions. In addition of the Agreed Definitions referenced in Section 1.2 of the Master Terms of Service, set out below or elsewhere herein are certain Agreed Definitions that are used in the Service Description and/or Specific Service Description, and if a definition in Section 1.2 of the Master Terms of Service is also set forth herein, the definition in such Master Terms of Service is merged into and supersede by the definition herein set forth with respect to Master Terms of Service as it applies to a Service One Offering:

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

"**Company Networks**" means Company's information technology networks, systems, devices, assets, files, information, data, and Trend Micro Technologies that must be accessed by Trend Micro in order to provide a Service One Offering, as may be specified by Trend Micro from time-to-time.

"**Critical Event**" means an event or status identified by Trend Micro from Company's deployed Trend Micro Technologies as being a potential cybersecurity threat to Company that requires further action or analysis by Company. To the extent that any Trend Micro Technology automatically blocks or remediates such potential threat, such threat will not be deemed to be a Critical Event.

"**Cyberthreat Data**" means any malware, spyware, virus, worm, Trojan horse, ransomware, or other potentially malicious or harmful code or files that Company does not want, as well as IP addresses, malicious domains and URLs, DNS data, network telemetry, commands, executable binary files, macros, scripts, processes or techniques, metadata, or other information or data associated with the foregoing, that may be related to unauthorized intrusions by any person or attacks by third parties associated therewith and that: (**a**) Company provides to Trend Micro in connection with Managed MDR Services; or (**b**) is accessed, collected, or discovered by Trend Micro during the course of providing any Managed MDR Service, excluding only the portion of such information or data that identifies Company or is the personal data of any human being that is regulated under any Applicable Law. Cyberthreat Data is not Confidential Information or Third Party Data hereunder.

"**General Service Description**" means description of the Service One Offering set forth herein that is applicable to all versions of Service One. This General Service Description is a Service Description for purposes of the Master Terms of Service.

"**Master Terms of Service**" means the Terms Of Service for Trend Micro Cloud Services published by Trend Micro and in effect on the effective date of purchase of a Service One Offering as evidenced in the Certificate, which Master Terms of Service govern and control the rights and responsibilities of the Parties with respect to the purchased services. The Terms Of Service for Trend Micro Cloud Services is published at trendmicro.com/eula or as may be requested by Company from legal_notice@trendmicro.com.

"**Required Access**" shall have the meaning set forth in Section 2.2.

"**Required Access Rights**" shall have the meaning set forth in Section 2.2.

"**Required Decisions**" shall have the meaning set forth in Section 2.3.

"**Service Description**" for each Service One Offering is comprised of: (**a**) this General Service Description EXCLUDING Schedule 1 when Service One Essentials is purchased by Company; and (**b**) this General Service Description INCLUDING those set forth in Schedule 1 and/or referenced therein when Service One Complete is purchased by Company.

"**Service One Complete**" means the services outlined in this General Service Description INCLUDING the services set forth in Schedule 1.

"**Service One Essentials**" means the services outlined in this General Service Description EXCEPT for those set forth in Schedule 1 that are only performed by Trend Micro for those customers purchasing Service One Complete.

"**Service One Offering**" means the following Service One services offered by Trend Micro: (1) Service One Essentials and (2) Service One Complete, that may be purchased by Company in connection with its deployment of Trend Micro Technologies.

"**SOW**" shall have the meaning set forth in Section 4.

"**Technical Services**" shall have the meaning set forth in Section 4.

"**Third Party Data**" means any files, information, and/or data concerning, belonging, or relating to a third party or to which such third party (including any human being) otherwise has rights to authorize, restrict, limit, control, and/or prevent further disclosure or processing under Applicable Laws; *provided, however*, the term Third Party Data does not include Cyberthreat Data of any kind or nature.

"**Trend Micro Technologies**" are separately-offered Trend Micro products and/or services that MUST be purchased, provided, and actively deployed by Company in order for Trend Micro to perform and provide the services (including, without limitation, Early Warning Services and Service One Complete if purchased) under such specific Service One Offering.

"**Work Product**" means all deliverables, data, information, reports, works of authorship, materials, inventions, and discoveries that are: (**a**) owned or licensed by Trend Micro or its affiliates or third party licensors prior to commencement of Services and/or the Pilot; (**b**) developed, acquired, conceived, or reduced to practice by Trend Micro (or its personnel or those persons acting on behalf of Trend Micro) during the provision of a Service One Offering; and (**c**) modifications, enhancements, and derivative works of any of the foregoing as part of or in the course of providing a Service One Offering and the Intellectual Property Rights therein. Work Product shall include, without limitation, identification of any Cyberthreat Data such as attacking IP addresses, malicious domains and URLs discovered by Trend Micro in the course of providing a Service One Offering as well as the detection, identification, blocking, removal, remediation, or resolution thereof. For clarity, "Work Product" does not include Company's Confidential Information.

2. Trend Micro Technologies. In order to receive a Service One Offering, Company must have valid licenses for, or be subscribed to, the required Trend Micro Technologies identified in Section 6.B.ii below, and if Company purchases Service One Complete, those identified in the applicable Specific Service Description at all times during the service since no software licenses or rights of use to any Trend Micro Technologies are granted under the Master Terms of Service or any Service Description or are included in the fees for any Service One Offering. Further, Company agrees to license and deploy the most current version and configuration of each Trend Micro Technology that is supported for a Service One Offering.

3. Intellectual Property.

3.1 Ownership of Work Product. As between the parties, all Work Product, and all Intellectual Property Rights worldwide therein or related thereto, is the exclusive property of Trend Micro, its Affiliates, and/or its or their licensors/suppliers. All rights in and to the Work Product not expressly granted to Company in this Agreement are reserved by Trend Micro, and Company will have no other or different rights (implied, by estoppel, or otherwise) or privileges with respect to any Work Product. Nothing in this Agreement does or will be deemed to grant, by implication, estoppel, or otherwise, a license under any of Trend Micro's existing or future patents or other Intellectual Property Rights. The Service One Offering will not be interpreted or deemed to be, and the Parties agree that the Service One Offering (and Work Product) do not constitute, "works for hire," "works made in the course of employment," "works made in the course of duty," or similar terms otherwise enforceable under Applicable Laws whereby the transfer of intellectual property rights or ownership created by an author occurs on the performance of services for an employer or customer. Trend Micro reserves the right to take any and all reasonable steps to prevent unauthorized access to, and use of, any Work Product by any person.

3.2 License from Trend Micro for Work Product. Trend Micro grants to Company a non-exclusive, royalty-free, fully paid-up, non-sublicensable, non-transferrable license, to use, display, and make a reasonable number of copies of the Work Product provided to Company by Trend Micro as part of the Service One Offering, solely and exclusively for Company's internal business purposes (and not for the business use or for the benefit of any person or third party other than Company).

3.3 License from Company. Company hereby grants to Trend Micro a non-exclusive, royalty-free, fully paid-up, sublicensable, transferrable license, in perpetuity, for all business purposes, to use, reproduce, distribute, display, create derivative works based on, and disclose to third parties all data and information provided or made available by Company or its personnel, contractors, or representatives or otherwise learned or observed by Trend Micro in connection with the Service One Offering regarding: (**a**) Work Product; (**b**) the detection, identification, blocking, removal, remediation, or resolution thereof; or (**c**) all logs and data, coming from the Company Network, whether from Trend Micro Technologies or Trend Micro tools or agents deployed within the Company Network. Except as required by Applicable Law, Trend Micro may not identify Company in connection with its disclosure of the data and information licensed to Trend Micro under this Section to third parties.

4. Installation and Configuration - Company Responsibilities. Company will install, configure, and set up, at Company's sole cost and expense, all Trend Micro Technologies and any other software, hardware, or other products, to ensure that all data and information necessary or advisable for Trend Micro to provide the Service One Offering is delivered and transmitted to, and received from Trend Micro, in the form, format, and timing identified by Trend Micro. Company understands and agrees that Trend Micro is unable to provide the Service One Offering to Company unless and until Company has fully and correctly licensed, installed/deployed, and configured all Trend Micro Technologies and any other software, hardware, or other products unless, and only to the extent that, Trend Micro provides such technical services by separate SOW as described in Section 5.

5. Technical Services by Trend Micro. In the event that Company requests that Trend Micro provide some or all of the necessary activation, installation, deployment, and configuration services for: (**a)** Trend Micro Technologies; (**b**) other software, hardware, or other products required in connection with Service One; or (**c**) any other technical assistance that Company may require in connection with its performance of its obligations hereunder (collectively **"Technical Services"**), any such

Technical Services shall only be provided by the Trend Micro Service One Operations team pursuant to the terms and conditions set forth in a separate statement of work if and as may be agreed by Parties at Trend Micro's then-current rates (each a "**SOW**").

6. Early Warning Service.

6.1 Overview. All Service One Offerings includes the following Early Warning Service. From time-to-time, Trend Micro may identify critical cybersecurity threats within Company's environment that may pose additional security risks to Company, and if identified by Trend Micro, inform Company of such additional threats. As part of this Early Warning Service, Trend Micro may use intelligence-driven (based on such things as threat intelligence reports, threat intelligence feeds, and/or malware analysis) or situational-awareness driven (suspicious events or indicators that happen on critical or high priority assets within the network) methods, processes, or analytics. Please note that Trend Micro does NOT perform any type of vulnerability scanning, penetration testing, or similar as part of Early Warning Service.

A. Trend Micro Responsibilities:

i. If Trend Micro identifies a critical event that may have an impact on Company's environment or believed to be part of an early stage of an attack, Service One engineers will inform Company via email or other designated contact method with the relevant details.

ii. Early Warning Service notifications will be provided to Company via email or via online tool.

B. Company Responsibilities:

i. Must specify desired contact and escalation points for alerts.

ii. Company must separately procure and deploy one or more of the following Trend Micro Technologies: Trend Micro Apex One, Trend Micro Apex One as a Service, Trend Micro Deep Security Manager, Trend Micro Cloud One – Workload Security, Trend Micro Cloud App Security, and/or Trend Micro Deep Discovery Inspector.

iii. Company must have the Smart Protection Network (SPN) feedback functionality enabled, as well as other Trend Micro best practice configurations such as, but not limited to, Predicative Machine Learning and Behavioral Monitoring enabled, in order for the Trend Micro Service One team to provide relevant feedback. Without SPN enabled, any feedback from Trend Micro will be limited to industry or macro-environmental level threats not specific to Company's network/environment.

iv. Company must also deploy Trend Micro Vision One and the associated Early Warning App in the product console. Company acknowledges and agrees that the Trend Micro Service One team will have access to Company's Vision One console in order to monitor threat indicators and other suspicious activity in Company environment and to facilitate follow-up recommendations with Company on suspicious events.

v. Cooperate and respond timely to requests for information and other assistance by Trend Micro to help Trend Micro identify in-scope threats to Company.

6.2 Onboarding and Deployment. Once an Order has being received and accepted by Trend Micro for the Service One Offering and acknowledged by the created and delivered Certificate, Trend Micro Service One Operations will, in an initial e-mail, request to schedule an initial onboarding call with Company. Once scheduled, the Service One Services team will provide Company with instructions in order to permit Company to configure Trend Micro Technologies for the specific purpose of the Early Warning Services component of Service One that has been purchased.

A. Trend Micro Responsibilities:

i. Provide instructions to Company to configure the deployed Trend Micro Technologies within the Company's environment to enable Early Warning Service functionality.

B. Company Responsibilities:

i. Enable outbound connectivity and accounts as needed to allow connection of Company's deployed Trend Micro Technologies to Trend Micro's Smart Protection Network.

ii. Implement Trend Micro's best practice configuration as outlined in this Section 6 in order to be eligible for any applicable Early Warning Service monitoring and notifications.

iii. Update Trend Micro Technologies in a timely fashion to newest version, including, but not limited to, application of Critical Patches and other fixes.

iv. Use and follow the required Trend Micro tools and processes to interact with the Service One Services team.

7. Proactive Advisory. In addition to the Early Warning Service, Trend Micro from time-to-time may also identify on-going high profile cyber-attacks that may not have any direct connection to Company's environment, but still may be of interest for Company's security staff. These Proactive Advisory notifications will be clearly differentiated from specific environment alerts found through the Early Warning Service and may be utilized by Company as it deems appropriate.

8. Periodic Health-Checks and Security Assessments. As part of the Service One Offering, Company may request up to two (2) consultations per year to review Trend Micro Technologies configurations as well as discuss general security practices assessment and recommendations that are applicable to Trend Micro Technologies only. For the avoidance of doubt, any security assessment hereunder is limited to an evaluation under Trend Micro's pre-defined checklist that evaluates Company's deployment of Trend Micro Technologies, tools, and technologies, but is not an assessment of Company's general/overall security posture, production network/environment, systems, or third-party software/services/products. Company understands and agrees that the consultation is general in nature only for Company's internal consideration only, therefore, all actions taken or not taken arising from or related to any such consultation shall be at the sole discretion and determination of Company and its management.

9. Priority Handling of Technical Support Cases. Company may use Trend Micro's designated online case management system to submit suspected malware cases or other service requests for resolution at any time. By completing a series of online forms, Company can provide Trend Micro and its authorized support representatives with key information necessary to begin addressing a malware case or Trend Micro Technologies problem. When Company submits a service request to Trend Micro via the designated online case management system, cases from Service One customers are given a higher priority over those customers not subscribed to Service One.

10. Priority Scheduling for Paid Incident Response Service Engagements. In the event of an internal major malware outbreak or other security breach or event, Company may request remote assistance from Trend Micro. Trend Micro will reasonably work with Company to triage and assess the extent of the issue. Depending on the severity and scope of the issue, Company may elect to engage with Trend Micro on a comprehensive separate Incident Response service to be provided under a separate fee-based Incident Response SOW. Once the Incident Response SOW has been agreed, Service One customers are given priority scheduling consideration.

11. No Use of Service One Offerings in a High-Risk Environment.

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

without limitation, reasonable legal, professional, expert, and attorney's fees and costs), indemnify, and hold harmless Trend Micro and its Affiliates, from and against any damages, losses, liabilities, costs, expenses or the like arising out of or related to any third party claims, demands, suits or causes of action of any kind or nature incurred as a result of, or arising out of, or relating to, in whole or in part, Company's deployment or use of any Service One Offering in a High-Risk Environment. The Parties agree that no limitation or exclusion from liability set forth in Section 8 of the Terms of Service shall limit the obligations of Company under this Section 11. The obligations of this Section 11 will survive any termination or expiration hereof and no limitation or exclusion from liability.

11.2 Section 2.9 of the Terms of Service. Trend Micro and Company agree that Section 2.9 of the Terms of Service is merged into and superseded by this Section 11 only with respect each Service One Offering purchased by Company hereunder.

12. Limited Warranty; Disclaimer of All Other Conditions, Guarantees, and Warranties.

12.1 Limited Warranty. DURING THE TERM, TREND MICRO WARRANTS TO COMPANY ONLY THAT IT WILL PERFORM EACH SERVICE ONE OFFERING PURCHASED BY COMPANY HEREUNDER IN A COMPETENT, WORKMANLIKE MANNER CONSISTENT WITH ANY GENERALLY ACCEPTED STANDARDS OF THE INDUSTRY. If at any time a Service One Offering purchased by Company does not conform to the foregoing Limited Warranty, and Company notifies Trend Micro in writing of such failure within the warranty period, Trend will use commercially reasonable efforts, at its sole cost and expense, to re-perform any non-conforming Service One Offering to achieve commercially reasonable conformance with the Limited Warranty; *provided, however*, the Parties specifically agree that Trend Micro shall have no obligation hereunder with respect to this Service Description: (**a**) to correct any or all defects, failures, and/or errors in Trend Micro Technologies; or (**b**) with respect to matters, events, or circumstances arising from or related to any other agreement between Parties or non-performance of any obligation of Company hereunder.

12.2 Disclaimer of All Other Conditions, Guarantees, and Warranties. EXCEPT AS SET FORTH IN SECTION 12.1 ABOVE, EACH SERVICE ONE OFFERING IS PROVIDED "AS IS, WITH ALL FAULTS" AND "AS AVAILABLE" AND WITHOUT ANY OTHER WARRANTY, CONDITION, UNDERTAKING, OR GUARANTEE OF ANY KIND OR NATURE. WITH RESPECT TO EACH SERVICE ONE OFFERING, TREND MICRO EXPRESSLY DISCLAIMS ALL REPRESENTATIONS, GUARANTEES, CONDITIONS, UNDERTAKINGS, OR WARRANTIES OF ANY KIND (WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE) ARISING FROM OR RELATED TO A STATUTE, CIVIL/COMMERCIAL CODE, CUSTOM, USAGE OR TRADE PRACTICE, COURSE OF DEALING OR PERFORMANCE, OR THE PARTIES' CONDUCT OR COMMUNICATIONS WITH ONE ANOTHER, OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AND/OR CONDITION OF: MERCHANTABILITY; FITNESS FOR A PARTICULAR (SUCH AS A HIGH-RISK ENVIRONMENT) OR GENERAL PURPOSE; TITLE; SATISFACTORY QUALITY; ACCURACY; NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS; OR ABILITY TO ACHIEVE A PARTICULAR RESULT. FURTHER, TREND MICRO DOES NOT REPRESENT, WARRANT, OR GUARANTEE THAT: (**a**) THE SERVICES AND FEATURES CONTAINED IN A SERVICE ONE OFFERING WILL MEET THE REQUIREMENTS OF COMPANY OR THAT A SERVICE ONE OFFERING WILL SATISFY ANY PARTICULAR BUSINESS, TECHNOLOGICAL, SERVICE, SECURITY, OR OTHER NEEDS OR REQUIREMENTS (SUCH AS USE IN A HIGH-RISK ENVIRONMENT) OF COMPANY; (**b**) USE OF A SERVICE ONE OFFERING WILL PROVIDE COMPLETE AND ABSOLUTE PROTECTION OF COMPANY'S SYSTEMS, NETWORKS, DEVICES, ASSETS, INFORMATION, AND/OR DATA FROM AND AGAINST ANY OR ALL CYBERTHREAT DATA OR OTHER POSSIBLE CYBER RISKS; (**c**) USE OF A SERVICE ONE OFFERING WILL DETECT, IDENTIFY, BLOCK, REMOVE, REMEDIATE, OR RESOLVE SOME, ANY, OR ALL CYBERTHREAT DATA; OR (**d**) A SERVICE ONE OFFERING WILL BE PERFORMED ERROR-FREE.

12.3 Section 7 of the Terms of Service. Trend Micro and Company agree that Section 7 of the Terms of Service is merged into and superseded by this Section 12 only with respect each Service One Offering purchased by Company hereunder.

SCHEDULE 1

SERVICE ONE COMPLETE

ADDITIONAL SERVICES

1. Service One Complete.

1.1 Overview. Service One Complete customers will be entitled to all of the services set forth in this General Service Description as well as the additional services described in this Schedule 1 hereto.

1.2 Managed XDR Services - Advanced. Service One Complete includes Trend Micro's Managed XDR - Advanced services whereby alert data is collected by Trend Micro Technologies and sent to Trend Micro's proprietary Managed XDR Platform (the "**Managed XDR Platform**") for analysis, and thereafter analyzed by security operation analysts (herein "**Managed XDR Operations**"). As part of each Managed XDR – Advanced service, Trend Micro: (**a**) monitors and reviews in-scope security events collected by the supported Trend Micro Technologies; (**b)** seeks to determine the root cause/entry point where possible, enrich event alerts where possible using threat hunting and investigation, and communicate known potential corrective action to a customer; and (**c**) where available, may suggest changes based on Trend Micro's knowledge in malware prevention. Trend Micro security analysts will be available to work directly with the Managed XDR - Advanced service customer online and via telephone from the Trend Micro security operation centers located around the world. The complete Service Descriptions for Managed XDR - Advanced services are included herein by reference and are made a part hereof for all purposes and are set forth at https://www.trendmicro.com/mdr-service-terms, each of which may be modified from time-to-time by Trend Micro at its sole discretion by publication of the revised Service Description.

2. Premium Support Program Services. Trend Micro Service One Complete Offering also includes the right of Company to receive the services and deliverables outlined in Trend Micro's Premium Support Program (PSP) agreement for Company's given Territory, with the following modification:

Service Manager. Depending on the Territory in which the company purchases Trend Micro Service One Complete, the operational title of the individual acting as the Service One Complete Service Manager for Company may be either referred to as a "Customer Service Manager" or a "Technical Account Manager" depending on Territory. For the avoidance of doubt, both titles are covered under the Service One Service Manager definition.

The complete Service Description for PSP provided in each Territory is included herein by reference and is made a part hereof for all purposes and published as follows:

Americas (including North and South America): https://www.trendmicro.com/nabupspcontract

Europe: https://www.trendmicro.com/eupspcontract

Asia, Middle East, and Africa: https://www.trendmicro.com/apacpspcontract

Trend Micro expressly reserves the right in each Territory to modify the Service Description for PSP from time-to-time at its sole discretion by publication of the modified Service Description at each URL.

3. Incident Response Engagement Request. In the event of an internal major malware, ransomware, or threat outbreak or other related security breach or event, Company may request an in-depth additional remote evaluation from Trend Micro's Incident Response (IR) Team in the form of a formal Incident Response Engagement Request, no more than once per annual contract year. All requests must be evaluated and scoped via a formal Statement of Work (SOW) by the Trend Micro IR Team, and Trend Micro reserves the final decision on whether or not an incident is covered under this service provision and the final scope. Services delivered under the annual Incident Response Engagement Request are limited to no more than forty (40) hours after acceptance by the Trend Micro IR Team and may not be carried over. Any services delivered past the initial 40 hours or separate incidents must be scoped under an additional SOW, which will be subject to an additional then-agreed fee at Trend Micro's sole discretion. All work delivered under this service will be done remotely via telephone and online tools unless specifically agreed otherwise. The Company and Trend Micro agree that the provision of IR Services is conditioned on Trend Micro having the competent resources then-available to provide such services. This service is provided on a best effort basis only,

and no guarantees can be made or are implied as to the outcome of the service. Trend Micro provides the final decision on the end of the engagement under this service.

A. Trend Micro Responsibilities:

i. Provide remote assistance and services up to 40 hours for a single approved incident.
ii. Provide communication updates and status reports to Company throughout the duration of the incident.

B. Company Responsibilities:

i. Identify main point(s) of contact for Trend Micro IR team engagement.
ii. Ensure Trend Micro IR team has the necessary access and permissions to conduct the work during of the engagement, including, but not limited to, any Company internal approvals.
iii. Provide prompt and complete information for IR team investigation as requested

C. Incident Response SOW: If Company and Trend Micro agree as a result of an Incident Response Engagement Request, the parties (at the sole discretion of each) will endeavor to develop and agree a SOW for additional Incident Response assistance to be provided to Company.