TREND MICRO DEEP SECURITY AS A SERVICE

SERVICE LEVEL AGREEMENT

1. Purpose

This document describes the services and conditions related to the Trend Micro Deep Security As Service and does not apply to, nor describes, any other Trend Micro product or service.

The use of the Trend Micro Deep Security As a Service is subject to acceptance of and agreement to the terms and conditions of the applicable License Agreement (the "License Agreement") of Trend Micro Incorporated or an authorized affiliate (each "Trend Micro"). This document shall be an integral part of such License Agreement. The terms and conditions of the Trend Micro License Agreement shall apply to the use of the Service described in this document. In the event of a conflict between the terms of the License Agreement and those of this document, those of this document will prevail. All other terms and conditions of the License Agreement will remain in full force and effect.

2. Service Description

The Trend Micro Deep Security As a Service is a server (VM or Instance) and application protection management service offered by Trend Micro and is referred to herein as the "**Service**". The Service provides protection and centralized security policy management for supported cloud providers. It also provides policy-based protection for servers running on IaaS cloud environments and combines a management console with software agents deployed in each cloud server. The Service allows customers to set rules based on the virtual machine information where the software agents are installed to check for specific virtual machine attributes.

3. Conditions of the Service

3.1 Customers must have an environment that has Internet access in order to use the Service.

3.2 Customers must ensure Firewall Access Control Lists (**ACLs**) are configured to allow communication from certain IP ranges as specified by the applicable documentation for the Service.

3.3 Customers must have access to a browser application supported by the Service to use the Web-based administrative console.

3.4 Customers understand and agree that their security policies and security events are also logged or recorded by Trend Micro.

3.5 Customers must take all necessary measures to ensure that they and all of their employees are aware of and in compliance with any requirements, responsibilities and limitations set forth in any applicable data privacy and data protection laws, rules, and regulations.

4 Service Availability

4.1 The Service is hosted twenty-four (24) hours a day, seven (7) days a week in Trend Micro's managed public IaaS environment. The Service systems, network, and capacity are continually monitored to provide optimal availability and efficiency to Service customers.

4.2 Subject to applicable law, Trend Micro may provide any part of the Service from any cloud provider data center (region) anywhere in the world. In addition, at any time and for any reason, Trend Micro may transfer the Service provided to the customer from one cloud provider data center to another. Trend Micro does not guarantee that any cloud provider data center, or part thereof, is dedicated to the sole use of the customer, unless otherwise specified in writing.

4.3 In connection with the registration of new Agents and assigning/updating security policies from the Deep Security Agent running on the customer's environment to the Service, "**Service Availability**" pertains to and means the Service's availability to receive heartbeat and communication requests from customer's Deep Security Agent, subject to the correct configuration by the customer of its firewall, as necessary, and other requirements and guidelines set forth in Trend Micro's applicable documentation.

4.4 Trend Micro is committed in providing the highest level of service available. Trend Micro's datacenter operates in multi datacenter availability zones with multiple redundant backup instances. Trend Micro will use commercially reasonable efforts to provide the Service on a 24 hours a day, 7 days a week basis. However, as described in this document, the Service may be unavailable due to Scheduled Maintenance, unscheduled downtime or unforeseen circumstances including suspension of the Service to mitigate any malicious activities; in each such case, Trend Micro shall use commercially reasonable efforts to reinstate the Service as soon as possible.

4.5 Scheduled Maintenance of the Service will occur periodically to ensure on-going efficiency. To the extent possible, Trend Micro shall give customers at least seven (7) days' notice of any "**Scheduled Maintenance**" which may cause disruption of the Service, including unavailability of the Service. Whenever commercially reasonable, Scheduled Maintenance will be conducted without affecting the Service provided to customers. Scheduled Maintenance shall not exceed more than eight (8) hours per calendar month. Whenever commercially reasonable, Scheduled Maintenance: (a) will be conducted during periods of anticipated low new activation requests or security policy creations/edits/updates request traffic and (b) will be conducted on part, but not all, of the network at any one time to minimize the disruption to the Service.

4.6 Unscheduled downtime is defined as those times when the Service is unavailable and not able to process new activation requests or creation/edit/updating of policy requests. This does not include those times when the Service is undergoing Scheduled Maintenance as described in section 4.5 above. Trend Micro will inform customers as quickly as possible following the onset of unscheduled downtime.

4.7 If at any time the continued availability of the Service would compromise the security of the Service due to, but not limited to, hacking attempts, denial of service attacks, or other malicious activities either directed at or originating from the customer's environment, Trend Micro may temporarily suspend the Service as to such customer. In such an event, Trend Micro will promptly inform the customer and will work with the customer to resolve such issues, reinstating the Service at the earliest opportunity.

5 Privacy Policy

5.1 Security event information communications are routed through the Service and are entirely automated so there is no human intervention.

5.2 As part of the Service account registration, the customer is required to provide their email address. The customer email address is used as the username to login to the Service and is stored

by the system.

5.3 To resolve a technical support problem, Trend Micro may request certain customer log files from the customer environment to help identify the problem. With the consent of and at the direction of the customer, Trend Micro may review such files to address customer's issue. Trend Micro will not otherwise access customer's files unless required by applicable law or pursuant to a court order or similar action.

6 Disaster Recovery

6.1 Trend Micro has a disaster recovery plan in connection with the Service. Because this is a Web-based Service, there may be events beyond the reasonable control of Trend Micro that may impact the Service ("Force Majeure Events"). However, to minimize the impact of these Force Majeure Events, the Service is based upon a geographically distributed, fully redundant system. If one data center becomes unavailable, the Service will fail over to a backup data center.

6.2 Disaster recovery procedures will be put into place under the following conditions:

6.2.1 A natural disaster or war situation that results in the primary data center hosting the Service not being able to serve customer requests for more than four (4) hours.

6.2.2 Any situation that results in the primary data center hosting the Service not being able to be accessed physically or remotely for more than four (4) hours by Trend Micro.

7 Technical Support and Customer Service

7.1 Customers may obtain technical support contact information by visiting the Trend Micro Deep Security As a Service support web page and selecting the appropriate region.

7.2 To receive prompt technical support, customer must provide the following information during the initial support call or email: Company Name, Administrator Account Name (but not the password), customer Contact Name, customer Contact Email Address, and a description of the issue. In addition, a copy of the license certificate should be included with online submissions (the license certificate information should also be available during phone support).

7.3 Customers that purchased a subscription to the Service through a channel partner should contact their channel partner for customer service requests regarding purchase order related queries, such as: (a) orders for the Service; (b) requests for modifications to the purchased service (*e.g*. changes to service management level, number of users, domains, etc.); and 3) billing and invoicing inquiries.

8 Modification

Trend Micro reserves the right to modify the Service and this document at any time without prior notice. The current version of this document can be found in the Trend Micro Deep Security As a Service administrative console for review by customers.