DEPENDENCIES AND ASSUMPTIONS

# Managed Security Services (MSS)

The agreement between the parties for MSS services was developed based on the following dependencies and assumptions, which if not accurate or adhered to, may require a change in the scope of services. Any change in services and fees will be mutually agreed to in writing by both parties. The dependencies and assumptions include:

- Trustwave shall not begin to provide the Services as described in the Order Form (OF) until Client has returned a signed OF and a Purchase Order (PO) for the total amount of the services selected (full contract amount). All terms and conditions included in a PO or submitted with a PO shall be null and void for all purposes.
- Client's primary point-of-contact (POC) as identified to Trustwave, or a designee, must be available to Trustwave during the entire engagement. The representative must have sufficient authority to schedule testing and address any issues that may arise.
- Client shall obtain all consents and authorizations from any third parties necessary for Trustwave to perform the Services, including without limitation, third party datacenters, co-locations and hosts. For the avoidance of doubt, Trustwave will not execute agreements with any such third parties
- The Service Level Agreements ("SLAs"), if any, for certain Managed Services described herein, which are incorporated into this Agreement and include commitments with respect to certain availability of those Managed Services, are set forth at https://www.trustwave.com/SLA/Ver001_Trustwave_MSS_SLA.PDF. The foregoing SLAs shall **no longer** apply to the following services:
    1) Security Technology Management (including added solutions)
    2) Security and Compliance Monitoring
    3) Managed Detection and Response for Endpoints
    4) Managed Unified Threat Management (UTM)
    5) Managed Intrusion Detection Security (IDS)
- The SLAs, if any, for the Managed Services described in 1-5 above, which are incorporated into this Agreement and include commitments with respect to certain availability of those Managed Services, are set forth at https://www3.trustwave.com/SLA/Ver003_Trustwave_MSS_SLA.pdf.
- To the extent that there are any inconsistencies between the SLAs posted in the service descriptions of 1-5 above and the SLAs posted for the services hereunder, the SLAs posted in this document will apply.

## Managed Security Client Obligations

- Client understands and acknowledges that Trustwave will rely upon the accuracy of any information provided by Client and that Trustwave's performance is dependent on Client's timely and effective satisfaction of all of Client's responsibilities hereunder and timely decisions and approvals by Client.
- Client shall provide, perform, and make available to Trustwave, at Client's expense within 30 (thirty) days of the Effective Date, the resources and actions and information set forth below, and such other additional resources and actions and information, as Trustwave may from time to time reasonably request in connection with Trustwave's performance of the Services.

Copyright © 2018 Trustwave Holdings, Inc. All rights reserved.

- Client agrees to cooperate with Trustwave in its efforts to gather initial technical and policy information required to establish the Service within 30 (thirty) days of Effective Date. Client will provide Client's current configuration and security policy information as reasonably requested by Trustwave.
- Client shall ensure that any computer equipment and hardware (and any replacement or substitute hardware or equipment), other than CPE supplied by Trustwave, shall conform to the specifications as provided to Trustwave.
- In the event remedial procedures are necessary, as determined by Trustwave in its sole discretion, Client will follow the reasonable instructions of Trustwave to effect such remediation.

Client will designate Authorized Persons to:

- consult with Trustwave on a regular basis in connection with the Services;
- cooperate with requests for information made by Trustwave related to the hardware, software, version, patch level, and configuration of devices connected to Client's network;
- assist Trustwave in upgrading and troubleshooting the CPE;
- grant Trustwave access to the Client's IP address(es) as identified and provided by Client to scan for open ports and other possible security vulnerabilities; and
- follow installation, configuration and/or maintenance instructions as provided by Trustwave.

- Client agrees to promptly notify Trustwave of any change in the authorization, contact information, or employment status of any Authorized Persons. Trustwave shall incur no liability resulting from Client's failure to provide such notification.
- Client will be solely responsible for any unauthorized acts or omissions that occur as the result of Client's access to or use of the Services or via the CPE and Client agrees to indemnify and hold Trustwave harmless from such acts or omissions.
- Client shall not distribute, reproduce, duplicate, copy, sell, resell or exploit the Services or any CPE for any commercial purposes or for the benefit of any third party.
- Client shall install and maintain all CPE delivered by Trustwave in an appropriate environment, with adequate power and environmental controls comparable to those generally considered appropriate for business computing equipment.
- Client shall not move the CPE to another network location unless it obtains approval in writing in advance of such move from Trustwave.
- Client shall provide Trustwave with at least five (5) business days' notice prior to taking any action that may affect the IP addressing of the CPE.
- Client agrees to make configuration changes to routers, firewalls (not managed by Trustwave), and other network devices upon Trustwave's request as required to enable communication between any CPE and Trustwave's SOC. If Client permits Trustwave to perform installation services via remote access, Trustwave shall not be responsible for any damages in connection with such remote access.
- If purchasing Managed Web Application Firewall Services, the following shall apply:
  - Client shall provide Trustwave with at least three (3) business days' notice prior to applying a significant change on the protected web application that will require re-base lining. The Client understands and acknowledges that a significant change to the web application requires a new base lining period and that failing to notify Trustwave in time could result in this taking longer than expected Client shall provide Trustwave with appropriate physical access to the CPE and to Client's site during normal business hours. Client will ensure Trustwave's ability to remotely access the CPE. Client agrees to promptly notify Trustwave prior to any planned outage of such access.
- If purchasing Cloud SIEM services, the following shall apply:

Copyright © 2018 Trustwave Holdings, Inc. All rights reserved.

  - Client shall provide access to Trustwave-defined netblocks to and from the CPE systems to collect data from, and provide health monitoring and platform management, of those systems.

- Client agrees to provide always-on Internet access to deployed CPE systems as specified by Trustwave. This refers to both outbound data sent from CPE systems to Trustwave's facilities, as well as inbound access from Trustwave as required to deliver each distinct service.
- For CPE deployed with out-of-band console devices, Trustwave strongly suggests Client provide an analog phone line dedicated to each out-of-band console so that Trustwave can respond to any outages or perform device maintenance where console access is required. If Client opts not to provide this access, Client accepts any delays in re-establishing service due to lack of console access.
- Client shall not modify, use or tamper with the CPE in any way, or to physically open or adjust the contents of CPE except as explicitly directed in writing by Trustwave or reverse engineer, disassemble or decompile any software loaded onto any CPE.
- Client shall document and promptly report all malfunctions of the CPE or interruptions to Trustwave's access of which it becomes aware. Client shall undertake any procedures reasonably specified by Trustwave necessary for the rectification of such malfunctions or interruptions within a reasonable time after such procedures have been received from Trustwave.
- Client will be solely responsible for providing the mechanism and storage location for any required data backups.
  - If purchasing managed SIEM Log Management appliance services, this will include all raw and parsed data stored in flat files on the SIEM Log Management appliance.
- Client shall not power off the CPE unless it obtains written approval in advance from Trustwave.

Copyright © 2018 Trustwave Holdings, Inc. All rights reserved.