Dependencies and Assumptions & Managed Security Client Obligations

All capitalized terms used in this document but not defined will have the meanings set forth in the applicable SOW or the Trustwave Master Terms & Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/. For the purposes of this document, "Equipment" has the same meaning as "CPE".

General Dependencies and Assumptions for All Services:

- Trustwave will not begin to provide the Services as described in a SOW or Order Confirmation, as applicable, until Client has returned the signed SOW or Order Confirmation and a purchase order ("**PO**") or purchase order exception for the total amount due under the SOW. All terms and conditions included in a PO or submitted with a PO will be null and void for all purposes.
- Client's primary point-of-contact as identified in a SOW, or another designee specifically identified to Trustwave, ("**POC**") must be available to Trustwave during the Term. The POC must have sufficient authority to schedule testing and address any issues that may arise.

Security Awareness Training Services Dependencies and Assumptions:

- Client is solely responsible for ensuring network bandwidth to access multi-media content, audio speakers, flash plug-in support, and supported browser versions.

Security Testing and DFIR Services Dependencies and Assumptions:

- Client will provide and coordinate Trustwave's onsite access to the systems being tested, as necessary. Before any system access is allowed, Client will inform Trustwave in writing and in advance of any security and access standards or requirements.
- During testing, the configuration of Client's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, then Client will inform Trustwave and a mutually acceptable testing schedule will be agreed upon.
- For testing support, Client will provide Trustwave with the following:
    - Names for the primary business and technical contacts
    - Restricted access to documentation and source code, if applicable
    - Last known good builds of product and tools on an as-needed basis
    - A process for input of bugs into the Client bug database and a template for bug reports
    - During business hours, best effort response time to help resolve any issues that may arise during testing.
- Trustwave may delete raw data and images ("**Evidence**") received from Client six (6) months after the issuance of any report relating to the Evidence.

Dependencies and Assumptions & Managed Security Client Obligations

Managed Security Services Dependencies and Assumptions:

- The Service Level Agreements ("**SLAs**") for certain 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 Descriptions and the SLAs contained in any SOW or MSA, the SLAs posted at the link above 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 in the SOW or Order Confirmation, as applicable, and timely decisions and approvals by Client. Client will provide, perform, and make available to Trustwave, at Client's expense, the resources, actions, and information set forth below, and such other additional resources, actions, and information, as Trustwave may from time to time reasonably request in connection with Trustwave's performance of the Services.

- Client will cooperate with Trustwave in Trustwave's efforts to gather initial technical and policy information as reasonably requested by Trustwave. Client will provide Client's current configuration and security policy information to and as reasonably requested by Trustwave.
- Client will ensure that any computer equipment and hardware (and any replacement or substitute hardware or equipment), other than Equipment supplied by Trustwave, will conform to the specifications as provided to Trustwave.
- If Trustwave determines that remedial procedures are necessary, Client will follow the reasonable instructions of Trustwave to remediate any issues.
- Client will designate authorized representatives 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 Equipment;
    - 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 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 representative of Client. Trustwave will 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 Equipment and Client agrees to indemnify and hold Trustwave harmless from such acts or omissions.
- Client will not distribute, reproduce, duplicate, copy, sell, resell, or exploit the Services or any Equipment for any commercial purposes or for the benefit of any third party.
- Client will install and maintain all Equipment delivered by Trustwave in an appropriate environment, with adequate resource allocations, including power and environmental controls, comparable to those generally considered appropriate for business computing Equipment.
- Client will not move the Equipment to another network location without advance notice and planning of such move with Trustwave.
- Client will provide Trustwave with at least five (5) business days' notice prior to taking any action that may affect the network connectivity or IP addressing of the Equipment.
- 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 Equipment and Trustwave's security operations centers. If Client permits Trustwave to perform installation services

via remote access, Trustwave will not be responsible for delays or other issues that may arise due to any failure to connect to Client's network with such remote access.

- Client will provide access to Trustwave-defined netblocks to and from the Equipment systems to collect data from and to provide health monitoring and platform management of those systems.
- Client agrees to provide always-on Internet access to deployed Equipment systems as specified by Trustwave. This refers to both outbound data sent from Equipment systems to Trustwave's facilities, as well as inbound access from Trustwave as required to deliver each distinct service.
- For Equipment 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 will not modify, use, or tamper with the Equipment in any way, physically open or adjust the contents of Equipment (except as explicitly directed in writing by Trustwave), or reverse engineer, disassemble, or decompile any software loaded onto any Equipment.
- Client will document and promptly report all malfunctions of the Equipment or interruptions to Trustwave's access of which Client becomes aware. Client will undertake any procedures reasonably specified as necessary by Trustwave for the rectification of such malfunctions or interruptions within a reasonable time after such procedures have been specified by Trustwave.
- Client will be solely responsible for providing the mechanism and storage location for any required data backups of Equipment.
    - If purchasing managed or co-managed client-dedicated SIEM services, Client will include all raw and parsed data stored on the SIEM.
- Client will not power off the Equipment unless it obtains written approval in advance from Trustwave.