MSSP AGREEMENT

Critical Start, Inc. ("Critical Start" or "MSSP") is a Texas based corporation located at 6851 Communications Parkway, Plano, Texas 75024. The following describes Critical Start's Service Level Agreements and Managed Security Service Provider terms and conditions for any organization ("Customer") using Critical Start's Managed Security Services ("Services").

This Critical Start Managed Security Services Provider Agreement ("MSSP Agreement") is based on information provided by the Customer about their external threats and known risks. The MSSP Agreement incorporates all terms and conditions from the Critical Start Master Services Agreement ("MSA"), which can be found at https://www.criticalstart.com/msa.

CRITICAL START AND CUSTOMER RESPONSIBILITIES

Incident Analysis & Response

Critical Start will provide detection, investigation, escalation and incident support for all incidents within the current supported toolset and visibility of the managed services. Task ownership underneath the function of Incident Response is outlined below using a RACI Model:

R
- Who is Responsible?
  - The person who is assigned to perform the work

A
- Who is Accountable?
  - The decision maker with ultimate ownership

C
- Who is Consulted?
  - Shareholders considered before a decision is made, or an action is taken

I
- Who is Informed?
  - The person who is informed about decisions or actions that have been taken.

Capability	Customer	Provider
Initial Incident Identification & Analysis	CI	RA
Initial Incident Investigation, Triage, and Classification	CI	RA
Incident Notification and Escalation	CI	RA
Initial Incident Mitigation & Response (Actions)	ACI	R
Escalated Incident Response & Investigation	RA	CI

Escalated Incident Forensic Analysis	RA	CI
Post-Mortem Analysis	RA	CI

Investigation and Escalation

Critical Start is responsible for incident detection, analysis, investigation, and escalation. It is the MSSP's primary responsibility to ensure that security events and incidents are detected and escalated in a timely manner. The MSSP will be the focal point for organizational security issues. The MSSP will be responsible for incident analysis and investigation to determine if alerts or security events warrant incident classification. If an event is classified as an incident by MSSP staff, the MSSP will be responsible for tracking the incident with the customer through final resolution. MSSP staff will perform incident triage to include determining scope, urgency, and potential impact, and will identify specific vulnerabilities and make recommendations to allow for remediation.

Critical Start will investigate all initial security incidents identified in ATAP and escalate as appropriate in accordance with the established and agreed upon Service Level Agreements (SLAs). All events and incidents will be analyzed and investigated using standard process and procedures. Escalations will follow established escalation paths and utilize contact information collected during on-boarding project(s), as mutually agreed by the parties and documented by Critical Start.

For incidents that are assigned to the Customer after analysis, the Customer is responsible for escalating incidents back to the MSSP that require action or analysis by the MSSP.

The MSSP will be the collection point for additional group inputs for classification of security incidents. The potential exists for other entities to notify the MSSP of possible events. In these relatively rare cases, the MSSP will ensure outside sources of information are incorporated into established MSSP workflow procedures. As events are pulled into the MSSP Workflow, it is the MSSP's responsibility to create and classify incidents. As the MSSP is responsible for incident escalation and response, only the MSSP has the authority to classify events or alerts as incidents to ensure due diligence of event investigation and accountability in reporting.

Additional responsibilities of the MSSP include:

- Perform analysis on customer assets/traffic, document results noting attacker profiles.
- Produce internal reports on security activity and MSSP workload metrics to include tickets opened, events per analyst hour, and open or pending items. Additionally, reporting may be conducted to demonstrate top firing incident types, top talking sources and destination and various other pre-determined MSSP metrics.
- Assist in identifying potential impact of incidents on customer systems and using available tools to assist customer in determining if data was exfiltrated.
- Document and track alarms (false positives and false negatives, blacklists, whitelists) within ATAP via Multi-Stage Filters, White lists, and Black lists.
- Escalate incidents to identified customer contacts for remediation.

Reports

Critical Start will provide reporting and metrics as mutually agreed by the parties, delivered on a monthly basis to pre-designated Customer personnel. This report will contain at a minimum, Event, Incident, and Investigation metrics as well as key performance indicators for associated technology effectiveness and analyst efficiency.

Advanced Threat Analytics Platform ("ATAP")

Critical Start will provide Security Event Orchestration capabilities using ATAP, including our Automated Classification Engine. This capability will provide event reduction, supervised learning, incident workflow and incident orchestration. Task ownership underneath the function of Security Event orchestration is outlined below using a RACI Model:

Capability	Customer	Provider
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development & Tuning	CI	RA
Incident Workflow & Notifications	CI	RA
Incident Orchestration	CI	RA
System Maintenance, Health & Performance	I	RA
Reporting & Metrics Development	CI	RA

SERVICE LEVEL AGREEMENTS ("SLA")

SLA Summary

Name	Description	SLA
SOC MSSP Portal Availability and Notification Systems SLA	Critical Start will provide access to the Advanced Threat Analytics Event Orchestration Portal, Splunk, and associated notification systems with the exception of "Scheduled and Emergency Portal Maintenance". System availability shall be measured by the number of minutes in the month minus the number of minutes the system is unavailable during the month to accept log feeds from Customer and process such data (adjusted for any scheduled downtime) divided by the total number of minutes in the month x 100.	99.9%
Individual Security Event Investigation SLA (TTD)	Upon generation of an alert that creates an incident, the Critical Start CyberSOC will begin investigation with the given timeframe after delivery to the Advanced Threat Analytics Event Orchestration Platform. The SLA timeframe in minutes is automatically calculated by the system and annotated in the audit log. This is measured by taking the difference between creation of the incident as shown in the audit log and when the incident is either assigned to a CyberSOC analyst or manually escalated.	60 minutes SLA Miss is available in Portal and Mobile SOC app
Weekly Median Incident Resolution Time SLA (MTTR)	TTR measures the total amount of time to resolve after an incident is created (t=0). This includes the delay to begin investigation (TTD) plus the total time spent for investigation and either escalation or close (TTI). For a weekly basis, MTTR will be calculated as shown in the MSSP Portal or in the Mobile SOC app.	60 minutes MTTR available in Portal and Mobile SOC app
Failed security event receipt notification	If a notification receipt failure occurs, the designated Customer contact(s) will be sent an e-mail notification and a time-logged phone call to the customer listed contact information for incidents within the SLA timeframe.	60 minutes
Executive Summary Reports	A monthly executive report will be delivered via email in Microsoft Word document format. This report will include all high-level summary information for the corresponding period.	Monthly

Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Critical Start of such failure. In order for Customer to receive a Service Level

credit, the notification of the Service Level failure must be submitted to Critical Start within forty-five (45) days of such failure.

SLA Metrics and Credit

The Monthly Service Fees referenced in the following tables excludes the service fees for any vendor product licenses.

SOC MSSP Portal Availability and Notification Systems SLA: 99.9%

System Availability	Credits Due Customer
99.8%-99.99%	No Credit Due
99.5%-99.79%	1% of the Monthly Service Fee
99.0-99.49%	3% of the Monthly Service Fee
98.5-98.99%	10% of the Monthly Service Fee
Less than 98.5%	25% of the Monthly Service Fee

Individual Security Event Investigation SLA (TTD): 60 minutes

Number of Incidents not assigned or escalated within 60 Minutes after the incident was created in the audit log	Credits Due Customer
5 or less	No Credit Due
6-10 Incidents	1% of the Monthly Service Fee
11-15 Incidents	3% of the Monthly Service Fee
16-20 Incidents	10% of the Monthly Service Fee
21 or More	25% of the Monthly Service Fee

Weekly Median Incident Resolution Time SLA (MTTR) : 60 Minutes

Median Time to Resolve (MTTR) measures the amount of time to resolve an incident, including the delay to begin investigation plus the total time spent for investigation and either escalation or close.	Credits Due Customer
1 Week > 60 minutes	3% of the Monthly Service Fee
2 Weeks > 60 minutes	10% of the Monthly Service Fee

3 Weeks > 60 minutes	25% of the Monthly Service Fee

Failed Security Event Receipt Notification to Customer: SLA: 60 Minutes

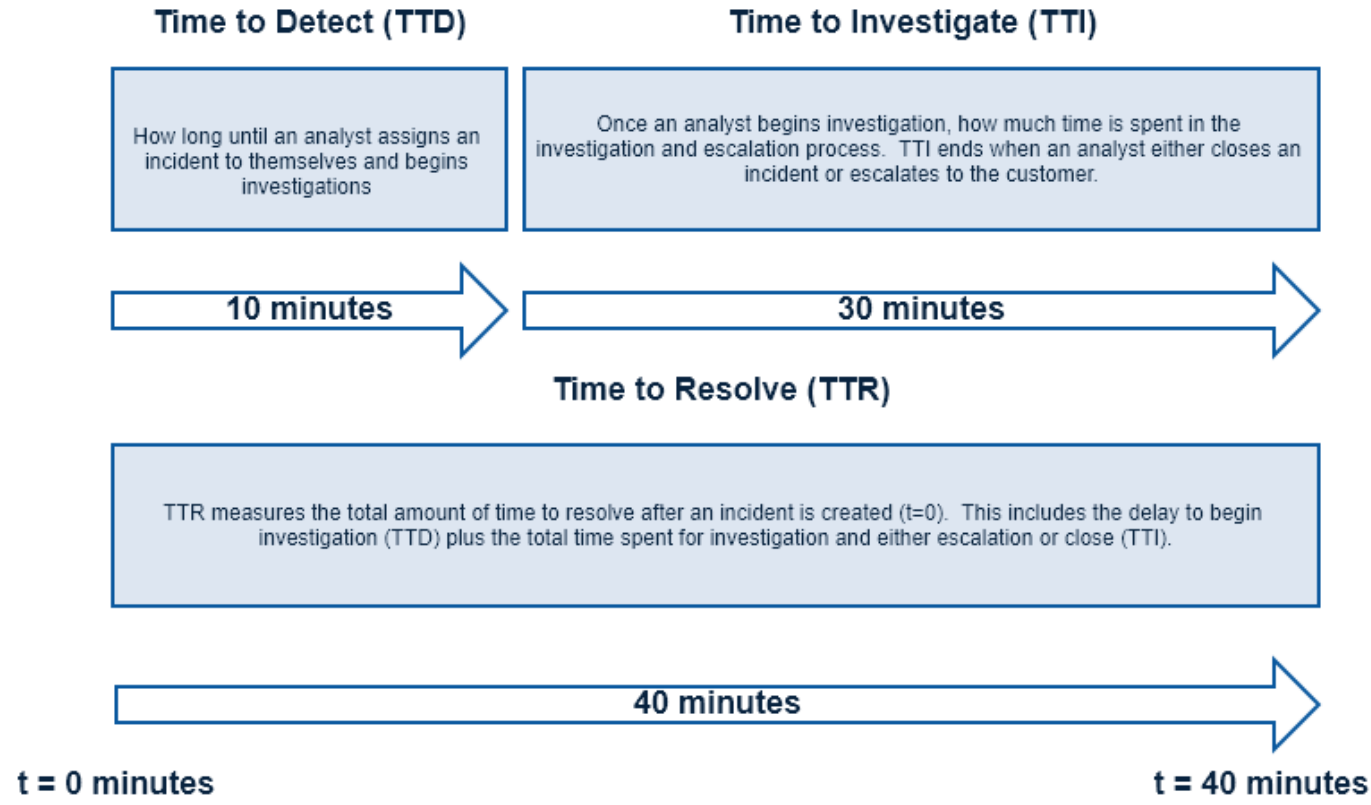
Number of Failed Security Event Receipts not escalated where Customer was not notified within 60 Minutes after occurrence	Credits Due Customer
5 or less	No Credit Due
6-10 Incidents	1% of the Monthly Service Fee
11-15 Incidents	3% of the Monthly Service Fee
16-20 Incidents	5% of the Monthly Service Fee
21 or More	10% of the Monthly Service Fee

Effective Date of SLA for Monitoring Services

Critical Start SLA's establish response time objectives and countermeasures for Security Incidents resulting from our MSSP Services. The SLA's become effective when the deployment process has been completed, the devices and security controls have been set to "live", and support and management of the devices and security controls have been successfully transitioned to MSSP Services.

The Customer will be notified in writing or via email that MSSP services have transitioned from deployment phase to full production monitoring.

Example of How Individual Incident Metrics Are Calculated



Credit Payment

Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to Critical Start of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to Critical Start within forty-five (45) days of such failure. Critical Start will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

If Customer pays the Fees annually in advance the credits due to Customer shall be paid to Customer in one of the following methods:

1) Credit to be applied to the next applicable invoice for the annual fees, or
2) In the form of a check to be paid to Customer within thirty (30) days after request by Customer

FILE ANALYSIS SUBMISSIONS AND ENDPOINT ISOLATION

Critical Start's MSSP has capability that will improve our ability to provide better analysis, detection and response to security threats that may impact customer environments. Our MSSP conducts dynamic and static analysis of unknown binaries and unknown files. This means that our analysts will be able to provide more in-depth analysis and context to their investigations of potential incidents, as well as enhancing the detection and prevention of future incidents that may involve the same file and/or binary. This function aligns with the mission of the Critical Start MSSP to further define "known good" and the unknown, therefore increasing our customers overall security posture.

Part of this new process may require our analysts to upload unknown binaries and/or files detected in Customer environments to dynamic sandbox and/or static analysis services such as VirusTotal and Palo Alto Networks WildFire ("WildFire"). VirusTotal ("VirusTotal") is owned by Chronicle Security Ireland Limited ("CISL"), an Irish Limited Company with registered number 507502, which is owned by Chronicle LLC, which is owned by Google's parent company Alphabet. At no point will Customer data and/or information be publicly exposed by the MSSP in this process.

Critical Start MSSP also has the ability to isolate machines on a Customer's network that have a supported endpoint EDR or endpoint protection solution as a part of their managed service offering. The MSSP uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Customer's network. If supported by the solution, the isolated machine will maintain connectivity to our MSSP and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks.

Unless Customer opts-out of File Analysis Submissions and Isolation services then Critical Start will upload potentially malicious files for analysis as needed and isolate endpoints investigation proves are potentially compromised.

Terms and Conditions for File Analysis Submissions

By allowing permission for the MSSP to upload unknown binaries, Critical Start MSSP servers will either manually or automatically upload unknown binaries to dynamic sandbox and/or static analysis services such as VirusTotal and WildFire:

- Each binary and/or hash and/or file metadata, as the case may be, will be submitted to VirusTotal and/or WildFire.
- Terms of Service and Privacy Policy of VirusTotal and/or WildFire will apply for each Customer.
- The MSSP shall not be responsible for this submission or for any act or omission by any online service.

You are hereby advised (i) VirusTotal makes the metadata publicly available along with scan results from dozens of anti-virus products and (ii) VirusTotal also makes the files available to VirusTotal partners. WildFire privacy policies are available at https://www.paloaltonetworks.com/resources/datasheets/wildfire-privacy-datasheet or directly from Palo Alto Networks.

Terms and Conditions for Isolations

Unless the Customer opts-out, Critical Start will isolate potentially compromised machines. Critical Start will manually isolate the machine using the EDR or endpoint protection solution and notify the customer of the isolation via the incident write-up procedure for escalation. The machines will remain in isolation until the

threat has been remediated or the customer has specifically said they accept the risk and request the MSSP to remove the isolation.

- The customer commits to identifying production impacting servers and assets that are NOT to be isolated unless the customer has given written authorization.
- The MSSP commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.
- The MSSP will escalate all incidents that required isolation to the customer for their visibility and active feedback on the incident.

Customers using EDR and/or endpoint protection solutions are hereby advised that the MSSP has the functionality to isolate machines on your network, that the MSSP has the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices on the network.

MANAGED SECURITY SERVICES GENERAL PROVISIONS

This Critical Start Managed Security Services General Provisions service description applies to all Critical Start managed security services. These general provisions are in addition to the specific terms and conditions provided in the services descriptions.

Customer Responsibilities

Customer understands that Critical Start's performance of the services is dependent in part on the Customer's compliance with the requirements of this SLA. The Customer understands that it is responsible for timely delivery of the items and information listed in the following sections of this SLA. Additionally, the Customer understands that it must perform the tasks, and provide access to Customer's employees, consultants, business processes, and/or systems as contemplated herein for Critical Start to be able to perform such services efficiently. The following list is required to ensure Critical Start's ability to perform the Services:

- Provide reasonable assistance to Critical Start for performance under this SLA, including helping trouble-shoot technical issues within the Customer's environment as well as any services provided by third-parties to the Customer that may affect the delivery of the Services.
- If applicable, provide a permanent, dedicated connection to support the Services. Customer is responsible for maintaining the functionality of the customer's components of this dedicated connection.
- Provide the necessary technical, license, and service information requested in the Pre-Installation Questionnaire (PIQ) prior to the commencement of Services.
- Develop a network map detailing relevant aspects of Customer's network architecture and delivering it to the Critical Start team for their reference when troubleshooting.
- Provide Critical Start with accurate and up-to-date information including, the name, email, landline, and mobile numbers for all designated authorized Customer Points(s) of Contact ("POC(s)"). Critical Start will also supply an accurate and up-to-date list of its POCs for Customer including name, email, landline and mobile number.
- Notify Critical Start at least seventy-two (72) hours in advance of any scheduled maintenance, network or system administration activity that would affect Critical Start's ability to perform under this SLA.
- Maintaining current maintenance and technical support contracts with Customer's software and hardware vendors for any device affected by this SLA.

Customer Environment Failures or Non-Performance.

Customer agrees that Critical Start will not be liable for any failure to provide the Services if such failure is caused by Customer's failure to meet the applicable requirements for each Service. At a minimum, Customer is responsible for ensuring the following environmental failures do not negatively impact the Services:

- Service interruptions, deficiencies, degradations or delays due to any Customer supplied internet or private access whether provided by Customer or third parties engaged by Customer, or equipment when provided by Customer or third parties engaged by Customer. Failure or deficient performance of Customer-supplied power, equipment, services or systems not provided by Critical Start.
- Customer's election to not release a service component for testing and/or repair and to continue using the service component.

- Customer's failure to adhere to Critical Start recommended configurations on managed or unmanaged equipment that affects the Service.
- Service interruptions, deficiencies, degradations or delays during any period when a service component is removed from Service for maintenance, replacement, or rearrangement purposes by Customers submission without a mutually agreed upon change order form.
- Failure to provide a suitable secure environment for on-premise devices, including, but not limited to: secure mounting/racking, appropriate cooling and air handling, premises secure from theft, loose wires bundled neatly, etc.

Service interruptions, deficiencies, degradations or delays in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform under this SLA that is under the management and control of Customer.

Testing of Monitoring and Response Capabilities

Customer may test Critical Start monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. Such activities may be initiated directly by Customer or by a contracted third party. Testing performed on newly added assets or data feeds should be communicated to Critical Start personnel via advanced electronic or written notice to ensure Critical Start personnel have properly onboarded new information and that all monitoring and response capabilities are working properly. SLAs will not apply during the period of such staged activities, and remedies will not be payable If the associated SLA(s) are not met for testing incidents.

Scheduled and Emergency Maintenance

Scheduled maintenance means any maintenance that is performed during a scheduled maintenance Window or in which Customer is notified at least five days in advance. Notice of scheduled maintenance will be provided to the Customer's Authorized Point of Contact.

Emergency maintenance means any non-scheduled, non-standard maintenance required by Critical Start.

No statement in the section of any Services Description entitled "Service Level Agreements" shall prevent Critical Start from conducting emergency maintenance if it is critically necessary for the integrity and security of the Services. During such emergency maintenance, Customer's Authorized Point of Contact will receive notification within 30 minutes of initialization of the emergency maintenance, and within 30 minutes of the completion of the emergency maintenance. Critical Start will be relieved of its obligations under the applicable SLAs during scheduled and emergency maintenance.

Network Server Change Notifications

Customer is responsible for providing Critical Start advanced notice regarding any network or server changes or outages to the managed services environment. In the event advanced notice cannot be provided, Customer is required to provide Critical Start with notification of changes within seven calendar days of such network or server changes. This applies to any assets which may affect the generation of and/or transmission capability of logs, and events or other activity which is monitored by Critical Start for Security Incidents. Unless otherwise specified in the Services Description, notification is completed by the submission or update of an inquiry ticket through the Critical Start Customer Portal for changes that will be implemented by Customer. For changes that

must be implemented by Critical Start, Customer must submit a policy change request ticket. If Customer fails to notify Critical Start as stated above, SLA remedies due to the identified change or outage do not apply.

Internet Emergency

In the event Critical Start declares an Internet emergency, it is Critical Start's objective to notify the Customer's specified Points of Contact via e-mail within 30 minutes of emergency declaration. This notification will include an incident tracking number and the time that Critical Start will conduct a situation briefing.

During declared Internet emergencies, Critical Start will provide a situation briefing and summarized e-mail designed to provide information that the Customer can use to protect their organization. Situation briefings following the onset of an Internet emergency will supersede any requirements for Critical Start to provide Customer-specific escalations for events directly related to the declared Internet emergency. During an Internet emergency, Critical Start will communicate all other priority level incidents, which are unrelated to said emergency, via automated systems such as e-mail, pager and voice mail.

Standard escalation practices will resume upon conclusion of the stated Internet emergency.

TERMS AND CONDITIONS FOR SOFTWARE

LIMITED LICENSE: The Customer must agree to not sell or transfer reproductions of the Service or any associated Products to third parties and to not use the Service or Products for any purpose not specifically permitted. This includes any vendor products and subscription services used to deliver the Service.

EFFECT OF EXPIRATION OR TERMINATION: The Customer must agree that promptly upon expiration or termination of the Customer Agreement, the Customer will delete all copies of the Product and all related materials. If the Customer received a CD or hard drive containing the Product, the Customer must agree to return the physical media to Partner. At software licensor's request, the Customer must agree to certify the destruction and return of the Product and related materials.

OWNERSHIP; COPYRIGHT: The Customer must acknowledge and agree that (a) title to the Product, and patents, copyrights and all other property rights applicable thereto, will at all times remain solely and exclusively with the vendor software licensor, and the Customer will not take any action inconsistent with such title, (b) the Product is protected by United States and other applicable laws and by international treaty provisions and (c) any rights not expressly granted herein are reserved to the vendor software licensor.

OTHER RESTRICTIONS: Except as expressly permitted by this Agreement, the Customer must acknowledge and agree that the Customer may not (a) cause or permit the disclosure, copying, renting, licensing, sublicensing, leasing, dissemination or other distribution of the Product(s) in this Agreement by any means or in any form, (b) use the Product to conduct a service bureau or similar business for the benefit of third parties, or (c) modify, enhance, supplement, create derivative work from, adapt, translate, reverse engineer, decompile, disassemble or otherwise reduce the Product to human readable form.

Ultrahazardous Activities: The Customer must acknowledge and agree that the Product is not designed, manufactured or intended for use in any environment in which the failure of the Product could lead to death, personal injury or severe physical or environmental damage, which uses and environments may include, but are not limited to, the design or operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines or weapons systems or the on-line control of equipment in any hazardous environment requiring fail-safe performance. The Customer must represent and warrant that the Customer will not install or use the Product for such purposes.

DISCLAIMER OF WARRANTIES: THE CUSTOMER MUST ACKNOWLEDGE AND AGREE THAT Critical Start SOFTWARE LICENSOR EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THE PRODUCT, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

EXPORT AND IMPORT COMPLIANCE: Customer must acknowledge and agree that (a) the Customer assumes the responsibility for compliance with all applicable import, export and re-export regulations, as the case may be, including but not limited to, any regulations of the Office of Export Administration of the U.S. Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, and other U.S. agencies and the export control regulations of the European Union; (b) the

Product will not be used, and none of the underlying information, software, or technology may be transferred or otherwise exported or re-exported to countries as to which the United States and/or the European Union maintains an embargo (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity 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"), which lists of Embargoed Countries and Designated Nationals are subject to change without notice; (c) the Customer will comply strictly with all applicable laws and assume sole responsibility for obtaining licenses to import, export or re-export as may be required; and (d) the Product may use encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations, 15 C.F.R. Parts 730-774 and Council Regulation (EC) No. 1334/2000.

GOVERNMENT RESTRICTED RIGHTS: Customer must acknowledge and agree that the Product is "commercial computer software" or "commercial computer software documentation", and that absent a written agreement to the contrary, the U.S. Government's rights with respect to such Product are limited by the terms of the Customer Agreement, pursuant to FAR § 12.212(a) and/or DFARS § 227.7202-1(a), as applicable.

THIRD PARTY BENEFICIARY: Customer must acknowledge and agree that vendor software licensor, and vendor software licensor's subsidiaries, are third party beneficiaries of the Customer Agreement with full power and authority to enforce the terms and conditions therein, and that, upon the Customer's acceptance of the terms and conditions of the Customer Agreement, the vendor software licensor will have the right (and will be deemed to have accepted the right) to enforce the Customer Agreement against the Customer as a third party beneficiary thereof.

INDEMNIFICATION: Both parties agree to defend, indemnify, and hold harmless the other, its officers, directors, employees, agents, successors and assigns from and against any and all claims, demands, losses, causes of action, damage, lawsuits, judgments, including attorneys' fees and costs, arising from or related to either's performance of its obligations under this Agreement, including, without limitation, allegations of damage to property, personal injury or death, except to the extent attributable to the negligent or otherwise wrongful acts or omissions of the other.