SERVICE ORDER ATTACHMENT FOR
SILVERSKY VULNERABILITY MANAGEMENT SERVICES (VUMA)

Capitalized terms not defined in this Attachment will have the meanings set forth in the MSA.

1. **"Services"** will mean SilverSky, as further defined in your order and incorporated herein by reference. The **"Launch Date"** of Services under this Attachment will mean the date on which Service(s) or any part of the services provided under the terms of this Attachment are first made available to you.

2. **Levels.** We will provide the Services pursuant to the objectives of the SilverSky Service Level Agreement set forth below.

3. **Customer Responsibilities.** During performance of the Services you will:
   I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Services;
   II. Ensure complete and current contact information is provided on a timely basis;
   III. Cooperate during the deployment period, including providing to us all required information in a complete and accurate form to prevent implementation delays which may result in additional fees;
   IV. Appoint one or more authorized contacts authorized to approve and validate all requested changes;
   V. Implement change requests; and
   VI. Provide all necessary information with respect to your environment.
   VII. Provide necessary hardware along with maintenance and support contracts to run log collectors within your environment.
   VIII. Send log data in an encrypted manner, or via the agreed log collection device/type.
   IX. Ensure that the format and quality of the data being sent to SilverSky is sufficient enough for SilverSky to provide the Services.

   You acknowledge that your fulfillment of these responsibilities is essential to our ability to perform the Services in a timely manner.

4. **Performance Evaluation.** You authorize us to evaluate service upgrades and changes on an annual basis at each of your locations which utilize the Services. In the event that such evaluations identify ways to improve performance or service at no additional cost to you, you authorize us to implement them.

5. **Term and Termination.** This Attachment will be in effect during the Initial Term set forth in *Appendix 1*, and will thereafter automatically renew for additional one year terms unless either of us provides the other with written notice of the intention not to renew at least 60 days prior to the beginning of the renewal term. Sections 1, 5, 6, 7, 8, and 9 of this Attachment will survive the expiration or termination of this Attachment for any reason. The provisions of the MSA that are identified in the MSA as surviving the expiration or termination of the MSA will, as they apply to this Attachment, also survive the expiration or termination of the Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, you must pay all fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

6. **Fees.** You will pay us the fees set forth in you order for Services you purchase. We will invoice you monthly except as may otherwise be indicated in your order. We reserve the right to increase fees on an annual basis if due to increases for the underlying technology or other general inflationary pressures.

7. **Cancellation Fee.** If this Attachment is terminated prior to the end of the Initial Term or any renewal term, for any reason other than our material breach of this Attachment or the MSA, you will pay us a cancellation fee. The cancellation fee will be equal to 100% of the greater of (a) your average monthly invoices or (b) the Minimum Fee, for the six months prior to the date of termination multiplied by the lesser of (x) the number of months remaining in the then current term of this Attachment or (y) 12 months. The cancellation fee constitutes liquidated damages and is not a penalty. You acknowledge that, if Services are cancelled prior to the completion of the Initial Term or any renewal term, SilverSky's damages will be difficult or impossible to ascertain. Your obligation to pay the cancellation fee is in addition to, and not exclusive of, your obligation to pay all fees accrued and unpaid at the time of termination for any reason.

8. **Additional Disclaimers.** We do not guarantee continuous, uninterrupted, virus-free or secure Services, and we are not liable if you or your end users are unable to access the Services at any specific time. We do not guarantee that we will be able to replace any of your information, content or other data that may be lost, damaged or stolen resulting from use of the Services.

SERVICE LEVEL AGREEMENT:
FOR VUMA

The following terms and conditions apply to the service levels of Services provided pursuant to this Attachment. In the event we fail to meet the levels defined in Service Level Agreement for a minimum of two (2) consecutive months, you must notify us in writing of any violations and allow us thirty (30) days from notification to cure the breach. If still unresolved, you may immediately terminate the Service giving rise to such breach without additional notification or incurring early termination fees within thirty (30) days of our failure to cure.

1. SERVICE HOURS OF OPERATION. We maintain Security Operations, Network Operations, and Technical Support departments on a 24 x 7 x 365 basis. You may reach an individual in each of these departments by calling the appropriate support service.

2. RESPONSE TIME. We commit to certain incident response times. These commitments are subject to your providing us accurate and current contact information for your designated points of contact. Our failure to respond in accordance with the parameters defined herein will entitle you to receive, as your sole remedy and our sole obligation, credits described below, *provided however*, that you may obtain no more than one credit per day, regardless of how often in that day we failed to meet these parameters.

2.1. Security and Network Operations Events. We classify all events as high, medium, or low level. We will identify or begin analysis of high level events within fifteen (15) minutes, medium level events within one (1) hour, and low level events within twenty-four (24) hours of occurrence. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 1 credit for high level events or one-day Tier 2 credit for medium and low level events.

2.2. Change Requests. We will make commercially reasonable efforts to begin implementation of changes you request to your service or equipment within twenty-four (24) hours of receipt of the appropriate change control form, requested changes will normally be implemented during Customer's non-business hours. Failure to respond in accordance with these guidelines will entitle you to a one-day Tier 2 credit.

3. SERVICE AVAILABILITY GUARANTEE. Our commitment is to have the Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Service(s) were not available to you in a calendar month (**"Service Unavailability"**). Service Unavailability will not include unavailability continuing for an hour or less or any unavailability that you fail to report to us within five (5) days. Failure to meet the service level described in this Section will entitle you to receive a Tier 1 credit.

4. MAINTENANCE. We reserve the following weekly maintenance windows during which you may experience periodic service outages:

(i) Tuesday and Thursday (12 AM – 2 AM ET)

(ii) Saturday (12 AM – 5 AM ET)

In the event we must perform maintenance during a time other than the service windows provided above, we will provide notification prior to performing the maintenance.

5. CREDIT REQUEST AND PAYMENT PROCEDURES. For failures to meet service levels herein in a calendar month, you will be entitled to receive a credit as specified below:

(i) **Tier 1.** Equal to twice the prorated portion of the monthly fee for the affected service; or

(ii) **Tier 2.** Equal to the prorated portion of the monthly fee for the affected service;

provided however that a breach of this SLA due to Exceptions described below will not qualify for such credits.

To receive a credit under this SLA, you must be current with your payments at the time Service Unavailability occurred. In addition, all credit requests must be submitted in writing, either through our ticketing system, via email or fax, or by certified U.S. mail, postage prepaid. You must submit each request for credit within seven (7) days of the occurrence giving rise to the credit claim. The total credit amount we will pay to you in any calendar month will not exceed, in the aggregate, half of the total fees invoiced to you for the Services for which a claim is made in the applicable month. (Credits are exclusive of any applicable taxes charged to you or collected by us.)

6. EXCEPTIONS. You will not receive any credits under this SLA in connection with any failure or deficiency of the Services or a failure to meet service level caused by or associated with any of the following:

(i) Maintenance, as defined above;

(ii) Fiber cuts or other such issues related to telephone company circuits or local ISP outside of our control;

(iii) Your applications, equipment, or facilities;

(iv) You or any of your end-user' acts or omissions;

(v) Reasons of Force Majeure as defined in the MSA;

(vi) Any act or omission on the part of any third party, not reasonably within our control;

(vii) First month of service for the specific Services for which a credit is claimed;

(viii) DNS issues outside our direct control;

(ix) Broadband connectivity.

7. FAIR USAGE CAP FOR LOG COLLECTION ON MONITORING SERVICE

(i) SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Monitoring Service. Failure to adhere to the fair usage policy will result in additional charges or a suspension of this SLA until such time as the usage level on the affected device falls below the notification threshold set forth below. Usage information is made available to you within the Security Management Console ("SMC").

1. SilverSky will notify you that you are exceeding the Fair Usage Threshold or "FUT" when you exceed any of the following FUTs:

   1. The average events per second across the set of monitored devices exceeds 10 events per second per device, over a 7 day period. An individual device exceeds an average of 100 events per second, over a 1 hour period

   2. The average events per second across the set of monitored devices exceeds 10 events per second per device, over a 30 day period.

(ii) Partial Service Suspension Threshold

Following the notice as set forth in (i) 7.1 above, if the average events per second across the set of monitored devices exceeds 25 events per second per device, over a 7 day period, SilverSky reserves the right cease ingestion of security events from an affected device, starting from the device producing the most events per second, until the average events per second across the set of monitored devices falls beneath the FUT.

Following the notice posted to the SMC as set forth in A.2 above, if an individual device exceeds an average of 250 events per second, over a 1 hour period, SilverSky may upon notification to the Customer cease ingestion of security events from the affected device.

Vulnerability Management

Service Overview

Vulnerability Management Services (referred herein as “VMS” or the “service”) delivers vulnerability assessments of Customer’s environment. VMS consists of automated and recurring vulnerability and compliance scanning.
VMS delivers vulnerability scanning and remediation data reporting of a Customer’s environment.
VMS provides unlimited scanning recurrence of Customer’s internal, external, and cloud-based live IP addresses. Scans of external IPs are conducted remotely. Scans of internal and cloud-based IPs are conducted from one or more ISO images placed on Customer’s network or in Customer’s leased virtual datacenter. IP level is based on Customer's technical scanning requirements.

Service Objectives: VMS service provides the customer with the following:

- Infrastructure scanning of the internal and external customer network infrastructure
- 24x7 Service support with online ticketing and alerting through the customer portal

Service Deliverables: VMS service will deliver to the customer the following:

- Agreed on list of IP addresses
- ISO image(s) for internal or cloud based IPs
- Customer portal access as well as ticketing system to view scan logs
- 24x7 SILVERSKY security support coverage

Service Description

Conduct scanning of the Customer infrastructure (for example servers, applications, network devices and end user devices) using a recognized industry vulnerability scanning tool , against the list of IP addresses as agreed, provided that those IP addresses are accessible from the Internet or through the supplied ISO image(s) and subject to the maximum numbers of IP addresses specified on the Order Form.
Scanning may be conducted as an ‘internal’ scan utilizing an ISO images within the Customer Network, as an ‘external’ scan utilizing a web based portal.
‘External’ scans can only be conducted on network assets and infrastructure with an internet-facing external IP address.
‘Internal’ scans can only be conducted on network assets and infrastructure that are accessible from the ISO images from its location within the Customer Network.

24x7 SOC Access

VMS Customers can contact SilverSky 24X7 via email or telephone. The Customer can use help desk calls for:

- Asking questions about the results of the Service, troubleshooting, or reviewing scan results, which will result in a ticket to the VMS SOC team.
- Changing contact information or rescheduling test dates and times.
- Solving issues associated with accessing the VMS service.
- Stopping scans during a network impacting event.

NOTE: Help desk calls cannot be used for general consulting advice that does not directly pertain to the results of the Service.

Vulnerability Reporting

We provide Customer with access to the Security Portal to view reports. Report capabilities are restricted to the capabilities of the platform and are Customer’s responsibility to generate.
Additional scan report result information is as follows:

- Vulnerability reporting with a description of each vulnerability, level of severity, business and technical impact, remediation suggestions, and links to relevant sites
- Discovery reporting, detailing live hosts discovered on the network
- Vulnerability remediation data

Security portal

We provide Customer with access to the Security portal. The Security portal may only be accessed by the named individuals specified by Customer. All information received by Customer through the Security portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

Profile Setup

We will assist Customer in selecting individual scan engine profiles as requested by Customer.

Customer Requirements

Customer agrees to perform the following obligations and acknowledges and agrees that SILVERSKY System's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer's compliance with the following:

VMS Delivery

The following procedures apply to the delivery of Vulnerability Management Services:

- Total IP quantities selected are limited to unique live IP instances and may not be rotated throughout the term of the contract for Customer accounts.
- Scan results and suggested remediation guidance are made available after the scan is completed.

Data Backups

The Customer acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Services or corruption or loss of data. The Customer agrees that it is Customer's responsibility to perform regular backups of all data contained in or available through the devices connected to Customer's IP address and/or domain names.

Cloud-Based IP Address Acknowledgement

The Customer acknowledges that the IP address of cloud-based assets is subject to change. The Customer agrees that it is Customer's responsibility to identify the specific IP addresses of cloud-based assets that are to be scanned.

Third Party IP Addresses: Authority and Indemnification

Except as set forth herein, Customer may use the Services only to scan the IP Addresses owned by and registered to Customer, or for which Customer otherwise has the full right, power, and authority to consent to have the Services scan and/or map. Customer may not rent, lease, or loan the Services, or any part thereof, or permit third parties to benefit from the use or functionality of the Service via timesharing, service bureau arrangements or otherwise. In the event one (1) or more of the IP Addresses identified by Customer are associated with computer systems that are owned, managed, and/or hosted by a third party service provider ("Host"), Customer warrants that it has the consent and authorization from such Host(s) necessary for SilverSky to perform the Services. Customer agrees to facilitate any necessary communications and exchanges of information between SilverSky and Host.