STATEMENT OF WORK FOR
NETWORK PROTECT SERVICES

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

1. **"Network Protect Services"** will mean SilverSky services including principal network security controls in a single-bundled package. This package includes Managed Firewall, Intrusion Detection Prevention Services (IDPS), Web Content Filtering, Gateway AV and remote access that includes two factor SSL VPN. SilverSky provides full management, monitoring and response for the services, access to configurable reports through the Security Management Console (SMC), and Lifecycle and Patch Management, as further defined in the *Order Form* attached hereto and incorporated herein by reference. The **"Launch Date"** of Network Protect Services under this Attachment will mean the date on which the Network Protect Services or any part of the services provided under the terms of this Attachment are first made available to you. or 45 days from the Effective Date, whichever date is earlier.

2. **Customer Responsibilities.** During performance of the Network Protect Services, You agree to perform the following obligations and acknowledge and agree that SilverSky's ability to perform its obligations, and its liability under the SLAs below, are dependent upon Your compliance with the following:
   - I. Prior to engagement commencement, assign a project management contact to serve as a primary contact through the delivery and performance of the Network Protect 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;
   - VI. Provide all necessary information with respect to your environment and communicate any network or system changes that could impact service delivery;
   - VII. Provide necessary hardware along with maintenance and support contracts to run log collectors within your environment;
     - a. You are responsible for ensuring that all customer provided hardware is not EOL and is able to support current software versions.
     - b. In the event of hardware failure of your owned equipment, You are responsible for initiating and fulfilling the return materials authorization ("RMA") process with the vendor and SilverSky
   - 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 Network Protect Services.

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

3. **SilverSky Deliverables.** During performance of the Network Protect Services, SilverSky will configure and deploy the selected security technology and will provide:
   - I. Continuous 24x7 device availability management (continuous health and security of your managed appliance)
   - II. A reporting platform to view and audit the alert response process (platform has integrated dashboards, incident management, and flexible reporting)
   - III. Service support 24x7 with online ticketing
   - IV. Threat intelligence correlation across the customer firewall and IDPS
   - V. A Security Management Center (SMC) Portal; portal with reporting functionality on Firewall, Web Content Filter, VPN and Intrusion Detection Prevention System (IDPS) logs
     - a. Management of Firewall policies includes Adding, deleting, or modifying individual Network Address Translations (NAT) (incoming, outgoing, and loop-back) including object creation
     - b. Adding, deleting, or modifying access control list changes (such as permit or deny changes) Including the creation of policy objects creation (Hosts, Groups, Networks, Ranges and Service objects)
     - c. Adding, deleting, or modifying individual network routes within the firewall
     - d. Adding, deleting, or modifying IDPS signatures, not including routine signature updates
     - e. Standard policy change may comprise one or more of the above bullets. SilverSky reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.
   - VI. Software Upgrades and Patch Maintenance (coordinated with the Customer)

a. In cases where support for a particular product or product version is being discontinued by the vendor or by SilverSky, SilverSky will communicate new platform migration options, if any. To be assured of uninterrupted service, Customer must complete the migration process within sixty (60) days notification by SilverSky.
b. For customer provided hardware, SKU S-xxx-3054, the Customer bears any costs relating to procuring new hardware or components and to re-provisioning any devices.
c. For customers who receive hardware as a part of their service, SKU S-xxx-3037, SilverSky will provide replacement hardware.

VII. Gateway Anti-Virus support (Fortinet). SilverSky will work with Fortinet to update anti-virus signatures/policies regularly when updates are released by Fortinet and reviewed by SilverSky.

VIII. Web Content Filtering (WCF) support (Fortinet). WCF as a licensed option is included in purchase of this bundle, SilverSky shall deploy the default categorization policy by zone or internet protocol ("IP") range as specified by the customer. Web sites that are accessed that are within an enabled category shall be blocked.
a. Customers can self-manage their WCF actions through the SMC portal or by sending in a change request to SilverSky Support. This is equated to a standard policy change request. Requests for whitelisting or blacklisting of domains are permitted under a standard policy change request

4. Performance Evaluation. You authorize us to evaluate service upgrades and changes on an annual basis at each of your locations which utilize the Network Protect 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. Equipment. Equipment provided to you by us **("SilverSky Equipment")** is for your use only during the Term of this Attachment. We will service the SilverSky Equipment in accordance with our service policies. You agree to (i) use SilverSky Equipment only for the purpose of receiving Network Protect Services; (ii) prevent any connections to SilverSky Equipment not expressly authorized by us; (iii) prevent tampering, alteration, or repair of SilverSky Equipment by any persons other than us or our authorized personnel; and (iv) assume complete responsibility for improper use, damage to or loss of such SilverSky Equipment regardless of cause. You will pay us for any damaged or unrecoverable SilverSky Equipment. You authorize us and our authorized agents, contractors, representatives, and vendors to enter your premises, with reasonable notice, during normal business hours (or as otherwise authorized by you), to install, maintain, repair and/or remove any SilverSky Equipment and/or to perform the Network Protect Services. You must return SilverSky Equipment, at your expense, within 14 days after this Attachment terminates or expires. SilverSky Equipment must be returned in the same condition in which it was provided to you, except for normal wear and tear. If you fail to do so, billing for Network Protect Services will resume and continue until all SilverSky Equipment is returned. Equipment for Network Protect Services delivered through us is maintained in a lockdown configuration that does not allow customer administrative access.

6. Term and Termination. This Attachment will be in effect during the Initial Term set forth in the *Order Form*, and will thereafter automatically renew for a period equal to the initial term as provided in the *Order Form*. The fee schedule listed in the *Order Form* will be subject to annual pricing adjustments however, such pricing adjustments may not exceed 5%, on an annualized basis, during the Initial Term. Intention not to renew must be provided at least 60 days prior to the beginning of the renewal term. The sections related to Payment Terms, Limitation of Liability, Warranties, Indemnity, Confidentiality and Intellectual Property from the General Terms and Conditions, as provided in the referenced General Terms and Conditions document, will survive the expiration or termination of this Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, you must pay all undisputed fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

7. Additional Disclaimers. We do not guarantee a continuous, uninterrupted, virus-free, malware-free, intrusion-free, or continuously secure Customer network or network environment, and we are not liable if you or your end users are unable to access your network at any specific time. Additionally, 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.

8. Network Protect is offered in two options, as defined below. The specific option chosen is detailed in the *Order Form*.

I. SilverSky provides the hardware bundled into the service:

SKU	*Description*
S-500-3037	SilverSky Network Protect up to 250MB thruput with FortiGate 60 Series
S-501-3037	SilverSky Network Protect up to 500MB thruput with FortiGate 80 Series
S-502-3037	SilverSky Network Protect up to 1GB to thruput with FortiGate 100 Series
S-503-3037	SilverSky Network Protect up to 3GB thruput with FortiGate 200 Series

II. Customer provides the hardware for the service:

SKU	*Description*
S-500-3054	SilverSky Network Protect up to 250MB thruput - no hardware included
S-501-3054	SilverSky Network Protect up to 500MB thruput - no hardware included
S-502-3054	SilverSky Network Protect up to 1GB thruput - no hardware included
S-503-3054	SilverSky Network Protect up to 3GB thruput - no hardware included

SERVICE LEVEL AGREEMENT FOR

NETWORK PROTECT SERVICES

The following terms and conditions apply to the service levels of Network Protect 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. **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.

   I. **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.

   II. **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. **NETWORK PROTECT SERVICE AVAILABILITY GUARANTEE.** Our commitment is to have the Network Protect Services available 99.5% of the time and as set forth below. At your request, we will calculate the number of minutes the Network Protect 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)
   III. 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;
   III. *provided however* that a breach of this SLA due to Exceptions described below will not qualify for such credits.
   IV. 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 Network Protect 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 Network Protect 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 Network Protect Services for which a credit is claimed;
VIII. DNS issues outside our direct control;
IX. Broadband connectivity.

7. **FAIR USAGE THRESHOLD FOR NETWORK PROTECT SERVICE:** When applicable, SilverSky maintains a fair usage policy to ensure the availability and sustainability of the Network Protect Service. Failure to adhere to the fair usage policy will result first in a notification to you and then, if you fail to take remedial action, suspension of this SLA until such time as the usage level associated with the corresponding data sources falls below a reasonable, standard threshold.