SERVICE ATTACHMENT FOR
EMAIL PROTECT SERVICES

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

"Services" will mean SilverSky Email Protect Services ("EPS"). EPS is a suite of services that includes Anti-SPAM, Anti-Virus (AV), Data Loss Protection (DLP), Targeted Attack Protection (TAP), Social Engineering Protection (SEP). EPS may also include Encrypted Email, quarterly security checkpoints and training & consulting.
Service SKUs:

- S-200-2884 SilverSky Email Protect User License
- S-200-2502 EPS Training - One Time
- S-200-2758 EPS Quarterly Security and Compliance Checkpoint
- S-200-2884 EPS Encrypted Email
- S-200-2758 EPS Quarterly Security Checkpoint Consultations (Essential Level)
- S-200-2502 EPS Training & Consulting

1. EMAIL PROTECT SERVICES. We will provide end users authorized by you to receive Email Protect Services (each a "**User**") with access to the Email Protect Services on the domain name(s) you specify to us, provided that you own the domain name(s). We will provision your specified domain names and Users on or before the date we first make Email Protect Services available to you ("**Launch Date**"). Additional domain names may be established thereafter.

2. ADMINISTRATORS. Prior to the Launch Date, you will appoint up to three administrators, each of whom will have the power to act as your agent, with the authority to make decisions and give notices on your behalf ("**Administrators**") and whose instructions and representations we may rely on. Administrators' authority includes, but is not limited to (i) controlling the creation and deletion of Users and domain names; (ii) managing changes to User information (such as changes to User name or password); (iii) serving as our authorized technical contact for the Email Protect Services; (iv) setting business rules/policies and/or filters on the Email Protect Services that may filter and/or terminate emails sent to or by Users without delivering them; (v) requesting the restoration or disclosure of content by submitting an Authorization for Disclosure of Information form to us, and (vi) monitoring complaints against Users. At least one Administrator must attend a training session on Email Protect Services, which we will provide at no charge. You may replace Administrators at any time upon notice to us.

3. TECHNICAL SUPPORT. You will have sole responsibility for handling technical support inquiries from your Users, unless you have purchased End User support from us. We will have responsibility for responding to inquiries from your Administrators regarding Email Protect Services. We will respond to inquiries from your Administrators on a 24x7 basis; provided that inquiries (i) must be submitted via toll-free telephone or email in the English language, and (ii) such inquiries will be responded to in English.

4. 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 the use of the Services.

5. ADDITIONAL TERMS. The following terms will apply to the Email Protection – Social Engineering Protection Services provided under this Attachment. These additional terms and conditions constitute your instructions to us to manually sample emails sent to or from Users to help us improve the performance of the Email Protection - Social Engineering Protection Services to you as described below. You may revoke these instructions at any time by following the opt-out process detailed below.

i. **DATA SAMPLING.** We will manually sample randomly selected emails sent to or from Users during the initial 180 days following the Launch Date ("**Sampling Period**") so that we may monitor and optimize the performance and effectiveness of the Email Protection - Social Engineering Protection Services to you ("**Data Sampling**"). A limited and controlled population of our or our Affiliates' personnel will be provided with automatically randomly selected emails (up to no more than 200 per day across all customers' emails processed through the Email Protection - Social Engineering Protection Services) for the sole purpose of monitoring and optimizing the performance and success rate of the analytics model deployed by the Email Protection - Social Engineering Protection Services, including by improving its detection ability (the "**Purpose**").

ii. During the Data Sampling Period, an Administrator may, in accordance with provisions below, revoke your instructions to perform Data Sampling. The Administrator may instruct us to stop Data Sampling with respect to any or all Users by using the sampling toggle switch (i.e., Social Engineering Sampling) on the Account Details page of the administration portal (the "**Sampling Selector**").

iii. The parties acknowledge that Customer Non-Public Personal Information (NPI) may be included in such randomly selected emails.

iv. Excluding any User(s) opted out by your Administrators, you warrant that your Administrators, acting on your behalf, are and will at all relevant times remain effectively authorized to give the instructions set out above on behalf of Customer and all Users.

v. We shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer NPI, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

vi. We shall cease processing the Customer NPI within 90 days upon the termination or expiration of this Services Order Attachment or, if sooner, the Service to which it relates and, subject to the preceding subsection, as soon as possible thereafter delete the Customer NPI from our systems.

vii. We may retain or disclose Customer NPI to the extent required by applicable laws.

Email Data Loss Prevention – Quarterly Security Checkpoint Consultations [Essential Level] S-200-2758

a. **Service Overview:** The SilverSky Email Data Loss Prevention (DLP) Security Checkpoint solution described below covers the ongoing quarterly consultative security reviews. As threats evolve over time, so will the techniques available to combat those threats. This solution is designed to enhance your ability to comply with regulatory and security requirements for email protection by leveraging automated policies on a continual basis to detect and prevent email data loss and/or leakage.

b. **SilverSky Deliverables:** The Deliverables are comprised of quarterly (i.e., once in every 3-month period) consultations with a Professional Services Security Consultant totaling up to two (2) hours each quarter.

c. Quarterly Security Checkpoint Consultative Review: A Security Consultant will work with you to determine a recurring quarterly schedule to perform your Security Checkpoint consultative session. Each quarterly review includes a collaborative performance review of up to an hour between you and a SilverSky Professional Services Security Consultant. During each collaborative review we will:

i. review the efficacy of your existing rules
ii. identify policy adjustments you may need to make
iii. provide new recommendations based on our knowledge of the current threat landscape

In addition to the collaborative review outlined above, another hour per quarter of consulting support will be available to implement any changes based on the findings in the performance review session. Unused consulting hours expire at the end of each quarter and will not carry over to subsequent quarters.

d. Customer Obligations:

i. Creating and managing your organization's specific business DLP rules/policies within the Security Management Console
ii. Managing the administrative quarantine (if applicable)
iii. Scheduling reviews and consulting support hours with a SilverSky Professional Services Security Consultant

e. Out of Scope:

i. End-User training
ii. End-User support from our Deployment team

f. Schedule:

i. The SilverSky Professional Services team is available to perform the described work above during the following business hours: Monday through Friday, 8 am MT – 5 pm MT - This excludes all SilverSky recognized holidays.

g. **Optional Additional Support:** Professional Services Security Consultant support services (in excess of the hours included in the solution as described above) will be available on an ongoing basis at the rate of $225 per hour (1 hour minimum). You must contact SilverSky customer support to arrange for additional consulting.

Email Data Loss Prevention - Training & Consulting SKU S-200-2502

a. **Service Overview:** The Email Protection Suite Training described below provides an overview of the tools available to email administrators to fully utilize the capabilities of the email protection solution. In addition, for customers with the Advanced Compliance solution, this training also covers the email DLP security policy administrative training which covers building, configuring, and managing

DLP policies. The objective is to help customers comply with regulatory and security requirements for email protection by leveraging automated policies to detect and prevent email data loss and/or leakage. This service is conducted during one live and interactive web-based training session which also includes a high-level review of applicable policies. Additional in-depth assistance with any of the items covered during the training and review can be addressed using additional Professional Services consulting hours. The SilverSky Professional Services team is available to perform described work above during the following business hours: Monday through Friday, 8am MT – 5pm MT - This excludes all SilverSky recognized holidays.

b. SilverSky Deliverables:

i. **Initial Assessment** Discuss the Customer's security and compliance profile to highlight features relevant to the customer. The training will be customized to address the specific customer requirements.

ii. **Training:** We will provide one live web-based training session covering the use of the Security Management Console (SMC). Training will include:
   a. Managing items in the quarantine/quarantine options
   b. Whitelists/Blacklists
   c. Key reports and information
   d. Logging & reporting
   e. Managing policies based upon "tests" and "actions"
   f. Managing lists
   g. Managing templates
   h. Managing disclaimers
   i. 'Monitor/log only' Mode best practices

c. Customer Obligations:

i. Creating and managing your organization's specific business rules/policies within the Security Management Console
ii. Managing the administrative quarantine (if applicable)

d. Out of Scope:

i. End-User training
ii. End-User support from our Deployment team
iii. Detailed assessment of customer's security and compliance requirements
iv. Consulting Support to set up policies to meet customer's security and compliance needs

e. **Optional Support:** Additional Professional Services consulting support can be arranged after the training on an ad-hoc or regular ongoing basis at the rate of $225 per hour (1 hour minimum). You must contact SilverSky customer support to arrange for additional Professional Services consulting.

Service Level Agreement for Email Protect Services

We are committed to providing a scalable and highly available solution through the following service commitment.

i. **SERVICE LEVEL AVAILABILITY CALCULATION**

$$\text{Availability} = \frac{\text{Total Monthly Minutes} - \text{Maintenance Minutes} - \text{Downtime Minutes}}{\textbf{Total Monthly Minutes} - \textbf{Maintenance Minutes}} \textbf{ X 100\%}$$

ii. **TERM OF THE SERVICE LEVEL AGREEMENT.** This Service Level Agreement becomes applicable to the Services upon the later of (a) completion of a mutually agreed upon stabilization period (if applicable), or (b) 30 days from the Launch Date.

iii. **DEFINED TERMS.** For the purposes of this Service Level Agreement, the following terms shall have the following meanings:

a. "**Available**" or "**Availability**" means that the Customer is able to access the Service via the specific access method for that Service subject to the exclusions defined in Downtime Minutes below.

b. "**Downtime Minutes**" means the total number of minutes that Customer's end users cannot access the specific Service via the normal access method for that Service. The calculation of Downtime Minutes excludes time a Service is not Available due to any of the following: (i) the Maintenance Minutes; (ii) your or your end users' own Internet service provider; (iii) a Force Majeure event; (iv) any systemic Internet failures; (v) (vi) third party encrypted email Services; (vii) any failure in your or your end users' own hardware, software or Network connection, (viii) your or your end users' bandwidth restrictions, (ix) your or any of your end users' acts or omissions; (x) you configure your email system to function as Open Relay; (xi) unavailability of your primary email service; and (xii) and each Service-specific additional exclusion stated below.

c. **"Filter"** means to detect and block or quarantine all email messages with viruses that (i) match against available/known virus signatures or (ii) are identifiable by industry standard heuristics.

d. "**Mail Delivery Time**" means the time elapsed between the entry of an email to our gateway and its exit.

e. "**Maintenance Minutes**" means the time period during which the Services will not be Available (i) each month so that we can perform routine maintenance to maximize the performance of the Services, up to 240 minutes (4 hours)per Service per calendar month, and (ii) any emergency maintenance we deem necessary in our sole discretion.

f. "**Maintenance Windows**" means the scheduled time period during which we might perform routine maintenance each week. Current Maintenance Windows are on Thursday from 10 PM to Friday 5 AM Mountain Time. We may change the Maintenance Window at any time. We will use reasonable efforts to notify you in advance of any changes to our normal Maintenance Windows.

g. "**Network**" means the network outside of our border routers.

h. "**Open Relay**" means an email server configured to receive email from an unknown or unauthorized third party and forward the email to one or more recipients who are not users of that email system. We reserve the right at any time during the supply of the Services to test whether the Customer's email systems function as an Open Relay. If at any time the Customer's email systems are found to function as an Open Relay, then we reserve the right to suspend all or part of the Services immediately and revoke SLA credit requests until the problem has been resolved.

i. "**Total Monthly Minutes**" means the number of days in the month multiplied by 1,440 minutes per day.

j. **"Virus"** means a known binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, or use inordinate system resources in the form of memory, disk space, or network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources.

iv. **MAINTENANCE NOTICES.** We will communicate the date and time that we intend to make Services unavailable through a global "welcome message" or an email sent to your Administrator at least 24 hours in advance or longer, if practical. You understand and agree that there may be instances where we need to interrupt the Services without notice in order to protect the integrity of the Services due to security issues, virus attacks, SPAM issues or other unforeseen circumstances.

v. **MEASUREMENT.** We use a proprietary system to monitor and measure whether the Services have met the Service Level metrics below and you agree that this system will be the sole basis for the resolution of any dispute that may arise between you and us regarding this Service Level Agreement. Our measurement system includes log files, database records and audit logs. We will make information we use to validate your claim available to you upon request.

vi. **SERVICE LEVEL METRICS - MEASURED ON A CALENDAR MONTH BASIS.**

a. **Availability**. The service level metric for availability is 99.99%.

b. **Mail Delivery Time**. The service level metric for Mail Delivery Time is an average of 3 minutes or less, subject to the exclusions defined in Downtime Minutes above and the following:

i. Exclusions

a. Delivery of email to quarantine
b. Delay associated with third party software (e.g., Microsoft Office 365)
c. Customer configuration rules for SPAM/AV or DLP
d. Initial 30 days immediately following deployment of our Anti-Virus Service

c. **Inbound SPAM.** The Service level metric for inbound SPAM detection is 99.5%

i. Exclusions

a. Not applicable to false negatives to invalid mailboxes
b. Customer is using less than our deployed default settings for SPAM and virus protection.

d. **Anti-Virus Service.** The Service level metric for Anti-Virus Service is 100%.

i. Exclusions

a. Cases of self-infection by the Customer
b. Binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware)
c. Virus-infected email that is quarantined but is subsequently delivered to an end user or administrator by releasing the message.
d. Emails containing attachments that are password protected, encrypted or otherwise under an end users control
e. The infection was determined to originate from a source other than inbound corporate email.
f. Customer is not employing our defined best practices at the time of infection:
g. Customer is not blocking or quarantining emails with encrypted compressed contents.
h. Customer is not blocking or quarantining known malicious files as defined by us.

VII. **AMOUNT OF SERVICE LEVEL CREDITS.**

Availability

Applies to: Email Security, Email Content Filtering, Email DLP

Availability	Amount of Credit for Affected Users for Affected Month
< 99.99% but ≥ 99.00%	25%
> 97.00% but < 99.00%	50%
< 97.00%	100%

Mail Delivery Time

Applies to: Email Security, Email Content Filtering, Email DLP

Mail Delivery Time (Consecutive Minutes Per Test Seat)	Amount of Credit for Affected Users for Affected Month
≥3 minutes but <10 minutes	25%
≥10 minutes but <15 minutes	50%
≥15 minutes	100%

Inbound SPAM Detection

Applies to: Email Security, Email Content Filtering, Email DLP Detection

SPAM Detection	Amount of Credit for Affected Users for Affected Month
<99.5% but ≥ 98.00%	10%

>95.00% but <98.00%	50%
<95.00%	100%

If SPAM is included with the mailbox, then the credit for SPAM will be 10% of the per mailbox monthly charge based on the table above.

Anti-Virus Service

Applies to: Email Security, Email Content Filtering, DLP, Anti-Virus Service

Virus Filtering	Amount of Credit for Affected Users for Affected Month
<100%	35%

VIII. REMEDY AND PROCEDURE. Your sole remedy and the procedure for obtaining your remedy in the event that we fail to meet the service level metrics set forth above are as follows:

You must notify us in writing at supportdb@silversky.com of both the date the Downtime Minutes occurred and an estimate of the amount of actual Downtime Minutes within five business days of our failure to meet the service level metrics (the "**Claim Notice**"). We will confirm the information provided in the Claim Notice within five business days of receipt of the Claim Notice. If we cannot confirm the failure to meet the service level metrics, then you and we agree to refer the matter to executives at each company for resolution. If we confirm that we are out of compliance with this Service Level Agreement, you will receive the amount of Service Level Credits above for the affected Service level metric and the affected Users for the affected month, which will be reflected in our invoice to you in the month following our confirmation of the failure.