STATEMENT OF WORK FOR
SILVERSKY MANAGED INCIDENT RESPONSE SERVICES

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

1. **"Services"** will mean SilverSky services including SilverSky Managed Incident Response Services "SilverSky MIR Services. The SilverSky MIR Service is provided in conjunction with your existing SilverSky Lightning MDR Service to reduce the time to detect, respond and recover from cyber incidents. The Statement of Work for SilverSky Lightning MDR Services is incorporated by reference. All terms, conditions, definitions, and descriptions from the Statement of Work for SilverSky Lightning MDR Services apply to the SilverSky Managed Incident Response Services unless otherwise noted herein. The two services together combine the key elements of incident response preparation, detection and analysis, containment and eradication and post-incident recovery into one solution. Incident Response Services are provided through SilverSky's partnership with our global Incident Response Provider "IRP". The IRP can be engaged via a start block of six (6) hours. The **"Operational Service Date"** of SilverSky MIR Services under this Attachment will mean the date on which the SilverSky MIR 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 SilverSky MIR 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. You will provide:
      A. A Project Liaison. You will designate an authorized representative to authorize completion of key project phases, assign resources, and serve as project liaison.
      B. Access. You will ensure SilverSky and IRP staff have access to key personnel and data requested.
      C. Resources. You will furnish SilverSky with your relevant personnel, facilities, resources, and information and perform tasks promptly.
      D. Cooperation. You will ensure your employees and contractors cooperate fully with SilverSky and IRP in a timely manner.
      E. Documentation. You will deliver, in a timely fashion, all documentation we request, including your security policies, network diagrams, server listings, and procedures, as applicable.

   II. In the event of a suspected incident, your responsibilities include:
      A. Declaration of the event as a formal incident and engagement of the incident response process. You will ensure your employees and contractors cooperate fully with SilverSky and IRP in a timely manner.
      B. Support the incident response process and provide any support, approvals, and decisions needed within the incident response process.

   III. In the event of an incident, your responsibilities include:
      A. Working with your cybersecurity insurance carrier to determine if they:
         a. Have a contractual relationship with IRP that allows IRP to be used to respond to the incident.
         b. Do not have a contractual relationship with IRP but will allow IRP to respond to the incident.
         c. Does not have a contractual relationship with IRP and requires you to contract with a different incident response provider that is not the IRP.

      Support the incident response process and provide any support, approvals, and decisions needed within the incident response process.

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

3. **SilverSky Deliverables**. During the performance of the SilverSky MIR Services, SilverSky will:

   I. Assign you a dedicated Cyber Security Advisor (CSA) who will:
      A. Hold regular meetings with you to baseline your cyber posture, assess your attack surface, and provide strategic recommendations to identify areas for risk mitigation and cyber posture improvements.
      B. Be your main point of contact for any compliance and security guidance.
      C. Assess the current state of your security program and provide strategic recommendations to strengthen your cyber posture.
      D. Assist you in developing a new Incident Response Plan or in making improvements to your existing plan.
      E. Meet with you (up to 5 hours annually) to perform a refresh and update to the incident response plan.
      F. Implement updates to the Incident Response Plan due to results of tabletop sessions and declared incidents (up to 4 hours annually).

II. Work jointly with IRP and your Cyber Incident Response Team to establish standard process flows around detection, investigation, performing temporary containment, incident escalation, response, forensic, and resumption processes.
III. Provide ongoing Incident Response Tabletop Exercises delivered through remote webinar testing sessions throughout the year. *Note*: SilverSky Professional Services can assist with updates to your Cyber Incident Response Team documentation through a separate Statement of Work.
IV. In the event of a suspected incident, we will
    A. Work with you to analyze the results of the event.
    B. Provide you with the information needed to determine if you would like to officially declare an incident and trigger the need for incident response.
    C. Work with you to utilize available technologies in place to provide temporary containment of the event.

IRP is responsible for:

I. Provide incident response support via the initial six (6) hours included in the retainer
II. Services for the Customer beyond the initial six (6) hours must be contracted directly with IRP

4. Key Assumptions

I. We will provide the MIR Services noted here via remote support.
II. You will provide us with reasonably requested information such as any existing Incident Response plans, incident response policies and procedures, and any other related documentation prior to the service kickoff call.
III. You will review your existing cyber insurance policy and any future renewals to validate that SilverSky and IRP are able to provide incident response services.
IV. You will provide access to personnel who understand your security policies, regulations, and requirements; such personnel will participate in the service kickoff call with our resources
V. You will evaluate our deliverables and immediately notify us of any perceived problems or issues with our obligations.
VI. We will immediately notify you of any perceived problems or issues regarding your obligations.
VII. The following items are out of scope for this Service:
    A. Any activity not explicitly included in this SOW is considered out of scope.
    B. In the event you request additional services, such services will be the subject of a change request.
    C. Full Incident Response Plan development outside of the elements outlined in this Service.
    D. Any additional managed services outside the scope of this Service.
    E. Onsite travel for participation in incident response activities.
    F. Additional Incident Response hours outside of the initial 6 hours in this Service.