SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-200-3154 VCISO SERVICE – TIER 3 "DEFENDER"

1. Overview

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement which incorporates this document by reference.

1.2 Service Background

SilverSky will assist the Customer by providing Virtual Chief Information Security Officer (vCISO) services to advise the leadership team and support the advancement of organization-wide cybersecurity measures, in accordance with industry best practices.

1.3 Scope of Services

SilverSky will assist the Customer by providing strategic program direction, oversight, and guidance to build and maintain a cybersecurity program. Defender delivers genuine embedded security leadership — approximately two days per week of active vCISO involvement. The full risk management cycle runs continuously, and enough time is available to sustain meaningful progress across 5–6 domains simultaneously. At this level, SilverSky Advisory is not a periodic reviewer; the vCISO is a working member of the security leadership team.

Project Component	**Parameters**
Minimum Contract Period	12 months
vCISO Hours / Month	40 hrs
Cadence	Weekly working sessions with security/IT team (60–90 min) + bi-weekly leadership or executive briefings
Reporting	Monthly KRI (Key Risk Indicator) dashboard + quarterly program health and roadmap progress report
Workflow Phases	Full cycle: Identify, Assess, Mitigate, Monitor, and Report — all five phases active each month. Quarterly roadmap review structures the Repeat phase.
Domain Focus	5–6 domains maintained actively; all domains remain in scope throughout
Ideal For	Mid-market companies scaling rapidly, operating in regulated industries, or with customers or insurers requiring a formal and evidenced security program

1.4 Representative Activities

At this tier, activities typically include some combination of the following, based on Customer's roadmap priorities and needs:

- Weekly working sessions — structured engagement with the security and IT team focused on active program execution, emerging issues, and roadmap progress
- Full risk register ownership and remediation tracking — maintaining a live, prioritized view of the organization's risk posture and actively driving remediation across the portfolio
- Security program advisory across 5–6 active domains — sustained engagement across risk management, governance, compliance, security operations, and other priority areas simultaneously
- Security awareness program guidance — advising on training design, phishing simulation programs, and staff communication strategy
- Audit readiness support — advising on evidence gathering, control documentation, and gap closure in advance of regulatory or

customer audits

- Tabletop exercise planning and facilitation — leading the organization through realistic incident scenarios to test response readiness (typically once per engagement year)
- Vendor due diligence — leading structured security reviews of key vendors and third parties as part of an ongoing supply chain risk program
- Monthly KRI dashboard — a data-driven view of the security program's key risk indicators, providing leadership with measurable evidence of risk reduction over time
- Framework and compliance alignment — advising on control mapping, gap remediation, and evidence requirements for NIST CSF, CIS Controls, ISO 27001, CMMC, or Customer's applicable framework
- NIST assessments, policy development, incident response planning, business continuity, and other structured advisory work as roadmap priorities and retainer time permit

2. Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If the Customer requests additional services, those services will be subject to a change request. Managed Services and ongoing operations of any program items are not included in the scope and will be outlined on a separate SOW.

3. Customer Obligations and Assumptions

Services, fees, and work schedules are based on the assumptions, representations, and information supplied by the Customer. The Customer's fulfillment of these responsibilities is critical to the engagement's success.

- Project Liaison - Designate an authorized representative to authorize the completion of key project phases, assign resources, and serve as project liaison
- Access - Ensure SilverSky consultants have access to key personnel and data requested - to include access to critical IT assets, systems and physical locations such as server rooms, data centers, and operations facilities
- Resources - Furnish SilverSky with Customer personnel, facilities, resources and information and perform tasks promptly
- Cooperation - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise the Customer if an increased level of Customer participation is required in order for SilverSky to perform the Services under this SOW.
- Documentation - Timely delivery of all documentation requested by SilverSky including Customer's security policies, prior security reviews, network diagrams, server listings and procedures

4. SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate and complete.
- Customer will provide access to Customer's personnel who have detailed knowledge of Customer's security architecture, network architecture, computer environment and related infrastructure.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky is unable to perform the Services due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

5. Project Parameters

5.1 Project Scope

The scope of the project is based on the above description with the additional details listed as follows:

Project Component	**Parameter(s)**
Project Start Date	Typically within 30 days of the Effective Date
Project duration	12 months
Project delivery method	Remotely via web meetings

6. Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.

[End of Document]