SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2029 NETWORK SECURITY ASSESSMENT

1 OVERVIEW

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

1.1 Service Summary

The purpose of the Network Security Assessment Service (the "Service") is to analyze, assess and test the overall design and integrity of the Customer network and critical information technology assets to uncover and identify potential security weaknesses and flaws. SilverSky will conduct this assessment onsite at designated Customer location(s).

SilverSky will examine existing Customer information security policies, security-related documentation and interview key personnel to assess the Company's overall level of network security and provide findings and recommendations regarding the level of compliance with regulatory and/or industry requirements. Following the assessment, SilverSky will provide an overview of results detailing the identified vulnerabilities or deficiencies and recommended steps to potentially remediate or mitigate the associated risk(s).

The foundational tier of the Service is a remote-only offering and as such covers a subset of the evaluation offered in the core and advanced tiers. Please see Section 4.1, "Project Scope," for a list of the evaluations included in each service tier.

Project Deliverables:

- Comprehensive Report

1.2 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement.

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Security Review
4. Security Testing
5. Analysis of Findings
6. Reporting

2 SCOPE

2.1 SilverSky Obligations:

Information Gathering Phase - Meet with key Customer staff to gain an understanding of the environment and network. SilverSky gathers existing network documentation such as server listings, network diagrams, device configurations, and network application listings, and examines documentation related to the Customer information security program, formal information risk assessment, and the current disaster recovery plan.

Security Review Phase - Review the network architecture and assess it against generally accepted industry standards and practices. SilverSky examines the overall network design and layout, including key aspects such as firewall policy, network segregation and utilization of security technologies, and operating system types and versions running on production equipment. SilverSky will interview key parties responsible for the implementation of and compliance with key regulatory or industry requirements to assess the extent to which existing policies and procedures have been implemented.

1. **Compliance Review -** Perform analysis of the security administration functionality and security program to assess high-level compliance with specific regulatory requirements (i.e., GLBA/Red Flag for financial institutions, HIPAA for healthcare providers, Reg S-P for investment firms) based on generally accepted industry compliance standards for particular regulatory requirements.

   The review typically addresses the following critical areas:

   - Security program development
   - Security roles and responsibilities
   - Risk assessment process
   - Access controls
   - Data security
   - Security monitoring
   - Incident response program
   - Change control
   - Business continuity and disaster recovery
   - End user security training
   - Vendor management

2. **Network Architecture Review -** Review the network and its overall design, setup, and layout with respect to security and compliance, based on generally accepted industry standards and practices.

   SilverSky reviews these critical components during this portion of the assessment:

   - Network segregation (VLANs, DMZs, subnets)
   - Security technologies (firewall, IDS/IPS, anti-malware solutions)
   - Firewall configuration
   - Wireless network review

- Gateways and entry points
- Network design

This review also includes conducting personnel interviews, performing system and network walkthroughs, and doing manual reviews and analyses.

3. **Physical Security Review -** Review security of hardware and media assets as well as primary and secondary physical measures used to protect those assets. This review will consist of personnel interviews and facility tours and walkthroughs. SilverSky analysis will compare Customer physical security against generally accepted industry standards and practices. (As noted above, the foundational level of this Service is conducted remotely; as such, this process is not included in that service level.)

   SilverSky's physical security review will address the following key areas:
   - Equipment placement
   - Physical access controls
   - Alarm systems
   - Surveillance/monitoring
   - Environmental controls
   - Climate controls (HVAC)
   - Handling of visitors
   - Backup systems

Security Testing Phase - Assess the integrity and overall level of security of critical network components such as servers and devices. SilverSky performs vulnerability scans, analysis of equipment configuration, manual checks, and other reviews of network components.

1. **External Network Assessment -** Perform vulnerability tests on the external network Internet routers, firewalls, VPN devices, web servers, and mail servers from an outside source to simulate what an actual attacker would be capable of seeing and doing on the network. Includes port scans to identify open network services followed by vulnerability scans to test if those services are susceptible to particular threats and exploits.

2. **Internal Network Assessment -** Assess components associated with the internal network and networked devices such as in-house servers, workstations, peripherals, switches, and routers. Do intensive testing on components considered "critical infrastructure" -- such as core servers and networking devices (routers, switches, etc.) and less intensive tests on non-critical components such as workstations and printers.

3. **Network Operating System –** Examine network operating system components such as user account setup, login and password settings, access rights to network applications and equipment, and audit settings, and assess against generally accepted industry standards and practices. Examples of common network operating systems are Windows Domain/Active Directory and Netware eDirectory.

4. **Host Security –** Assess and evaluate security controls in place at the individual server or system level which are specific to the individual host ("Host Security") (such as security patch levels, local account setup, file/directory security, and audit settings) and compare those controls to generally accepted industry standards and practices.

Analysis of Findings Phase – SilverSky will compile the data generated from review and testing, analyze it, and prioritize findings according to their criticality and potential impact and develop recommendations to potentially address risks associated with the vulnerabilities. SilverSky will also compare the overall security posture to compliance requirements and perform a gap analysis to identify specific deficiencies and areas targeted for improvement.

2.2 Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report comprised of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after a joint review with the Customer.

Executive Summary - The executive summary summarizes the results of the assessment. It is intended for upper management and the Board of Directors and includes:

- Overview of assessment results
- Itemization of the risk ratings for each area reviewed during the assessment
- Key findings and recommendations

Detailed Findings - The detailed findings section describes the assessment results in detail. It's designed for management, administrators and other operations personnel and includes:

- An itemized listing of the individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely for each vulnerability
- Affected resources
- Recommendations for remediation

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. In the event that the Customer requests additional services, such services will be the subject of a change request.

3 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

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

3.1 Customer Obligations

- **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
- **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 increased Customer participation is required in order for SilverSky to perform the Service under this SOW.
- **Documentation** - Deliver in a timely fashion all documentation requested by SilverSky including Customer's security policies, network diagrams, server listings, and procedures

3.2 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 security architecture, network architecture, computing environment, and related matters.
- 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 Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

4 PROJECT PARAMETERS

4.1 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	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 2-3 weeks, subject to project variables
S-266-2029 Network Security Assessment (onsite) - Tier 3	Organizations with less than 1000 Users. Work hours not to exceed 80
S-266-2029 Network Security Assessment (onsite) - Tier 2	Organizations with less than 500 Users, Work hours not to exceed 60
S-266-2029 Network Security Assessment (onsite) -- Tier 1	Organizations with less than 100 Users, Work hours not to exceed 40
S-266-2029 Network Security Assessment (remote) -- remote exercise	Organizations with less than 100 Users, Work hours not to exceed 30

4.2 Location and Travel Reimbursement

The Service defined in this SOW may require onsite participation by SilverSky staff at Customer location(s).

For Customer-approved onsite participation, the Customer will be invoiced for all actual SilverSky staff travel and living expenses associated with all onsite visits. An administration fee of ten percent (10%) of all travel and living expenses will be billed to Customer in the event Customer requires an itemized statement of such expenses.

Location	**Scope of Work**

4.3 Acceptance

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