1 OVERVIEW

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

1.1 Service Summary

The purpose of Web Application Penetration Testing (the "Service") is to identify the feasibility of an attack on a Customer's Internet-facing web application(s) and to determine the extent of the impact of successful exploitation of that intrusion. The testing will employ intrusion analysis and testing methodologies to test the potential for successfully exploiting weaknesses within your web-based applications. The process will mimic typical attacker techniques and actual attempts to exploit web application vulnerabilities.

SilverSky web application penetration testers will meet with key members of the Customer's staff to determine the scope and 'rules of engagement' for performing the testing according to the list of potential in-scope activities listed below. This includes finalizing expectations and determining specific aspects such as the extent and depth of testing, notification requirements, and the timing of testing. All web application testing is performed remotely with minimal time commitment from the customer during the testing phases. If any critical vulnerability is identified, SilverSky's testing team will notify the Customer's main point of contact as soon as possible while the testing is in process.

1.2 In-Scope Service Details

SilverSky's Level 2 Web application service consists of a Static Code Analysis testing of a customer's in-scope web applications. Static Code Analysis (also known as SAST) is a method of evaluating the security of an application's source code without executing the code. The analysis is performed by automated tools that scan the code, identify potential vulnerabilities and security issues, and report on the findings. Since this testing interfaces with the application's codebase, source code weaknesses that traditional GUI testing would miss may be identified.

The scope of the testing will be adjusted based on the specific need of the customer, but it may include the following options:

- Testing of one or more codebases
- Authenticated or unauthenticated testing of the applications
- Web application or mobile application testing
- Timebox or comprehensive level of effort

1.3 Project Summary

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

1. Kick-off Meeting
2. Static Application Security Testing (SAST)
3. Exploitation and Vulnerability Validation

4. Analysis of Findings
5. Draft Report and Review of Initial Findings
6. Final Comprehensive Report

1.4 SilverSky Methodology:

Kick-off Meeting – The purpose of the kick-off call is to discuss and agree on customer goals and the rules of engagement for the project. This includes project scoping (determining the target systems to be included in the testing), testing style (authenticated versus unauthenticated and the privilege level of authentication for users provided), the timeframe for testing, the extent to which system exploits can be performed, and procedures to follow should any issues occur during the testing. Any additional precautions or provisions are also considered before testing.

Static Application Security Testing (SAST) - Use automated toolsets to perform web application scanning of the targets. This includes information gathering techniques, port and service scans, fingerprinting and enumeration of systems. Once this information is gathered, the test will evaluate the security of an application's source code without executing the code. SilverSky will run automated tools that scan the code, identify potential vulnerabilities and security issues. SilverSky, during this phase, will assess the interfaces within the application's codebase and evaluate any source code weaknesses deeper into the application's source code.

Vulnerability Validation - SilverSky will make a best effort to validate findings from the application vulnerability scan manually. SilverSky processes and techniques for manual validation will vary significantly depending on the type of weakness identified but may include screenshots, manually verifying ports and protocols, or vulnerable versions in use. SilverSky will perform testing only under the agreed-upon rules of engagement.

Analysis of Findings Phase – SilverSky will compile and analyze the data generated from the assessment tools and manual checks and categorize vulnerabilities by severity, depending on the potential impact each can have on the affected network. This analysis is the basis for recommendations to address the risks potentially associated with the vulnerabilities.

Draft Report and Review of Initial Findings

At the conclusion of the assessment, SilverSky will provide a comprehensive draft report composed of an executive summary and a detailed findings section. The Customer will have an opportunity to review drafts of the report and make any comments on findings.

Final Report Delivery

SilverSky will deliver a final version after a joint review with the Customer, and any changes will be addressed from the draft report.

- Comprehensive Report detailing
    - Methodology followed.
    - Successful exploitation of the web application
    - Detailed recommendations for improvements

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope.

- Any web applications not identified as in-scope

- Any retesting of the application after remediations are addressed unless specifically included in the SOW scope.
- Any testing not outlined in the in-scope testing section

If the Customer requests additional services, such services will be the subject of a change request.

2 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 success of the engagement.

2.1 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 Customer increased Customer participation is required 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

2.2 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 understand 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.

3 PROJECT PARAMETERS

3.1 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 2-4 weeks, subject to project variables; comments on findings preliminary to comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
Project Scope -Level 2 Static Code Testing Tier 1	Web App Penetration Testing – Static Code Testing up to 40 hours of testing.
Project Scope -Level 2 Static Code Testing Tier 2	Web App Penetration Testing – Static Code Testing up to 80 hours of testing.
Project Scope -Level 2 Static Code Testing Tier 3	Web App Penetration Testing – Static Code Testing up to 120 hours of testing.

3.2 Location and Travel Reimbursement

The Service defined in this SOW does not require onsite participation by SilverSky staff at Customer location(s).

3.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW. All deliverables will be marked with a Draft designation until final payment is received by the customer.