SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3150 M365 SECURITY AND CONFIGURATION ASSESSMENT

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 Services Summary

Microsoft 365 has become a critical tool for most organizations since it delivers all sorts of business services, from email to cloud storage. The M365 suite provides access to various tools that streamlines organizational workflows and provides the freedom to work from anywhere. This has provided an increasing need for organizations to ensure their deployment of M365 is secure and configured according to security and Microsoft best practices.

SilverSky's M365 Security and Configuration Assessment assures organizations that their M365 deployment has been configured to protect the business from potential security threats. The primary objective of the assessment is to identify any misconfigurations or weaknesses in your M365 configuration that threat actors could exploit within your environment. The Assessment covers several areas, including a configuration assessment against the industry security benchmarks such as CIS and Microsoft 365 security best practices. A secondary objective of the assessment is to review your current feature set usage of M365 to provide guidance to potential tools and features within your licensing tier of M365 that you may not be utilizing today.

Microsoft Office offers this product as part of a shared responsibility model in cloud computing. This means that Microsoft as the Cloud provider is responsible for cloud security. However, you as the Tenant or organization are responsible for your security in the cloud. As tenants, you have control of user accounts, access, authentication, and authorization of M365 data. Therefore, it is the customer's responsibility to maintain the security of their sensitive data. SilverSky's M365 review will help provide that assurance.

Benefits of a SilverSky M365 Security and Configuration Review:

- Ensure that the secure email strategy is effective.
- Validation of Office 365 security controls.
- Ensure strong authentication and data encryption practices.
- Sufficient logging and monitoring to ensure readiness for cyber security incidents.
- User permissions review and add-ons review.
- Review security controls against account takeover cyber-attacks and ransomware.

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. Controls Review
4. Analysis and Documentation
5. Reporting

1.3 SilverSky Obligations:

During the Office 365 security review, SilverSky will assess cyber security best practices, including but not limited to the following security review areas:

- Accounts and authentication policies
- Email cyber security configuration review and Exchange Online Protection
- Mobile Device Management Areas
- Data and secure storage management
- Application permissions
- Auditing configuration & monitoring controls
- M365 Active Directory related security concerns

Kickoff Call – SilverSky will perform a kickoff call to understand your environment and determine the best action to assess the customer's M365 tenant components.

Information Gathering Phase - This will cover security response processes and external controls that are not discoverable via the collection script or in your Office 365 tenant.

Review and Interactive Knowledge Transfer Phase - During this phase, SilverSky will review the following areas and provide recommendations and knowledge transfer on what was identified.

- Exchange Online Protection
- Zero-Day Threats
- Sender Authentication
- Simulating and Mitigating Phishing Attacks
- Data Retention and Deletion
- Auditing and Reporting
- Miscellaneous Email Risk
- Identity Management
- Authentication and Authorization
- Multi-Factor Authentication & Conditional Access
- Azure Identity Protection
- Device Management
- Microsoft 365 Groups

- Enterprise Applications ·
- Account Compromise Remediation
- Principle of Least Privilege

Analysis and Documentation Phase - SilverSky will compile and review the information gathered, then analyze and document in detail the findings and any test results in a draft iteration of the final reports.

Reporting Phase - All findings will be compiled into a report that includes issues and misconfigurations, potential paths to exploitation in Active Directory, and recommendations for remediation.

1.4 Deliverables

SilverSky will provide a Detailed Findings Report following its review.

The Detailed Findings Report describes the review results in detail. It is intended for mid-level management, administrators, and other operations personnel and includes:

- Itemized listing and description of the areas reviewed.
- Identified deficiencies.
- Overall risks associated with deficiencies.
- Detailed recommendations for addressing deficiencies.

Other deliverables that may be included:

- Knowledge Transfer Deck
- Remediation Planning Worksheet
- Management-level Closeout Presentation

1.5 Out of Scope

Any activity besides the items bulleted below not explicitly included in this SOW is considered out of scope. If the Customer requests additional services, such services will be the subject of a change request.

- Troubleshooting current issues in the environment
- Executing technical tasks, implementing changes, or remediation of the findings (SOA Remediation offering is available for the latter)
- Architecture or design review

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 can access key personnel and requested data.
- **Resources** - Furnish SilverSky with Customer personnel, facilities, resources, and information and perform tasks promptly.
- **Cooperation** - Ensure all the Customer's employees and contractors cooperate fully and promptly with SilverSky. SilverSky will advise the Customer if an increased level of Customer participation is required for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely delivery of all documentation SilverSky requests, including the Customer's security policies, network diagrams, server listings, and procedures.

2.2 SilverSky Assumptions

- The Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- The Customer will provide access to the Customer's personnel with detailed knowledge of the Customer's security architecture, network architecture, computing environment, and related matters.
- The Customer will provide access to the Customer's personnel who understand the Customer's security policies, regulations, and requirements.
- The Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify Customer of any perceived problems or issues regarding Customer's obligations.
- Customer is responsible for any additional costs if SilverSky cannot perform the Services 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 Scope	Assessment of a single Microsoft 365 tenant
Project Start Date	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 1 week, subject to project variables
M365 Security and Configuration Assessment	Includes assessment of (1) one M365 tenant. Not to exceed 60 hours of assessment work

3.2 Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely and do not require any onsite travel.

3.3 Acceptance

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