



## SERVICE ATTACHMENT

### SILVERSKY AWARE™ SERVICES

---

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

1. **“Service”** will mean SilverSky Aware™ Security Awareness Training and Phishing Testing. The Service is a fully managed security awareness and continuous training program which can satisfy regulatory compliance mandates (i.e., PCI, HIPAA, SOX, and FFIEC). SilverSky partners with KnowBe4 to provide and deliver this Service via our SilverSky Cyber Security Advisory team (CSA). Service SKUs:
  - S-200-3028 SilverSky Aware User License
  - S-200-3061 SilverSky Aware User Compliance Add On License
  - I-200-3028 SilverSky Aware User License Installation Fee
  - I-200-3061 SilverSky Aware User Compliance Add On License Installation Fee
2. **Customer Responsibilities.** During performance of the Service, you agree to perform the following obligations and acknowledge and agree that SilverSky’s ability to perform our obligations in a timely manner are dependent upon your compliance with the following:
  - I. Customer will:
    - A. Provide a technical resource familiar with your environment to assist in the implementation and testing during the initial setup of the services. This resource will assist with items such as providing:
      - i. An understanding of your specific regulatory and compliance requirements
      - ii. Your current information security documentation
      - iii. Your employees with access to related documentation
      - iv. Relevant information needed to configure your users
    - B. Participate in all scheduled reviews (as established, monthly, quarterly, annually)
    - C. Assume responsible for the onsite enforcement and follow-up to ensure user compliance and completion of all required trainings.
3. **SilverSky Deliverables.**
  - I. Deliver the Service via our SilverSky Cyber Security Advisory team (CSA), which will integrate threat intelligence and real-time attack profiles to provide training and testing using current social engineering tactics being leveraged by attackers.
  - II. Utilize threat profiles are based on SOC (Security Operations Center) metrics, industry research and customer risk profiles.
  - III. Build a custom security testing program that considers your desired testing frequency, internal department factors, industry risk profiles and any customization necessary for your business.
  - IV. Facilitate a complete user security awareness training suite.
    - A. This training suite is regularly updated to ensure users are current on the latest phishing techniques
    - B. Training content can be customized for targeted at-risk groups such as privileged users, executives, and security personnel.
  - V. Implementation of the Service will utilize defined process, coordinated by a specifically named project coordinator.
    - A. The SilverSky Compliance team will work with you on a monthly, quarterly, and annual cadence for phishing/social engineering testing and awareness training.
    - B. Specific deliverables for each phase will be communicated in the implementation process.
  - VI. Provide 8x5 support of the platform and manage ongoing support issues.
4. **Key Assumptions/Exclusions.**
  - I. Specific users will have limited access to administrative functions but based on their role in the system, will have the ability to login to perform trainings, review reports or managed sub functions as needed.
  - II. Excluded from this offering
    - A. Industry specific compliance trainings such as GDPR, HIPAA, PCI, or other compliance level trainings
    - B. Any service support after business hours
    - C. Phishing testing in excess of 4 quarterly sessions
5. **Additional Disclaimers.** We do not guarantee a continuous, uninterrupted, virus-free, malware-free, intrusion-free, or continuously secure Customer network or network environment, and we are not liable if you or your end users are unable to access your network at any specific time. Additionally, we do not guarantee that we will be able to replace any of your information, content, or other data that may be lost, damaged, or stolen resulting from use of the Services.