# SERVICE SPECIFIC TERMS
# PHISHING

These Service Specific Terms shall govern Client's use of the Phishing Services set forth on the applicable Order Form between the Client and Smarsh. Unless expressly stated otherwise, capitalized terms contained herein shall have the meaning given them in the Agreement.

Client's use of the Phishing Services is subject to Client's compliance with the following terms:

1) **PHISHING SERVICES.** The Phishing Services provided by Smarsh are designed to provide the Client with access to the following core functionalities:

   a. **Targeted Phishing Campaigns:**
      i. Client selects a phishing email template from the phishing campaign catalog.
      ii. Smarsh will initiate the email campaign using the selected template to its licensed users.
      iii. Client's licensed users will receive the phishing campaign email.
   b. **Activity Logging:**
      i. The following user events are observed and logged:
         - Email delivered to licensed user
         - Email opened by licensed user
         - Link within email clicked by licensed user
         - Email reply by licensed user
         - Email attachment opened by licensed user
         - Data submitted by licensed user
         - Email reported by licensed user
   c. **User Training:**
      i. Licensed users who record a failing status for the phishing campaign are required to complete phishing awareness training.

2) **RESTRICTIONS.**
   a. **Usage.** The Phishing Services are sold on an annual, per user basis. Each twelve (12) month period within Client's Subscription Term shall include four (4) phishing campaigns, delivered once per business quarter.
   b. **Scheduling.** Client will be responsible for initiating the scheduling of Phishing Services and determining the content and scope of the campaign, and failure to do so within the applicable Service Term will result in the expiration of the phishing campaigns purchased for the Service Term.

3) **CLIENT OBLIGATIONS.**
   a. Client is required to whitelist the domains and IP addresses from which phishing campaigns will originate. A list of domains and IP addresses, and instructions to assist in whitelisting, will be provided to Client upon initiation of a phishing campaign request.
   b. Clients must provide proof of ownership for all email domains included within phishing campaigns. This is accomplished by adding a TXT record provided by Smarsh to the DNS records for each domain.

4) **DEPLOYMENT LOCATION.** Unless agreed otherwise by the Parties in writing, the Phishing Services are deployed in a service environment or data center located in the United States.

5) **SERVICE DOCUMENTATION.** Smarsh will make available to the Client the Phishing Services Documentation in Smarsh's support portal - http://central.smarsh.com ("Documentation"), including any performance constraints or service guidelines, as amended from time to time, or directly upon written request.

6) **DISCLAIMER; LIMITATION OF LIABILITY.** EXCEPT AS EXPRESSLY SET FORTH ABOVE, THE SERVICES ARE PROVIDED "AS-IS" AND SMARSH DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. SMARSH SPECIFICALLY DISCLAIMS ANY AND ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, UNINTERRUPTED USE, AND ANY WARRANTIES ARISING FROM CONDUCT OR COURSE OF DEALING. SMARSH MAKES NO WARRANTIES OF ANY KIND THAT THE SERVICES WILL BE ABLE TO OR ACTUALLY SOLVE, IMPROVE, OR OTHERWISE MITIGATE ANY PROBLEMS CLIENT MAY EXPERIENCE WITH PHISHING OR ANY OTHER COMPUTER- OR CYBER-ATTACKS. SMARSH'S CYBER COMPLIANCE SERVICES (INCLUDING THE PHISHING SERVICES AND ANYTHING ASSOCIATED THEREWITH) IS NOT AN ANTIVIRUS, ANTIMALWARE, OR OTHER CYBERSECURITY APPLICATION; SMARSH WILL HAVE NO OBLIGATION TO UNDERTAKE EFFORTS TO ACTUALLY PREVENT OR MITIGATE ANY POTENTIAL OR REAL ATTACKS.

7) **CONFLICT.** To the extent that any language contained in the Agreement conflicts with any language contained in these Service Specific Terms, the terms herein shall control in connection with the Phishing Services.

8) **SUB-PROCESSORS.** The Phishing Services may rely on the Sub-Processors set forth in the Sub-Processor Exhibit attached hereto.

# PHISHING SERVICES

## SUB-PROCESSOR EXHIBIT

**Sub-Processor(s).** With respect to the Phishing Services, the following entities are sub-processors:

| Name | Location | Role |
|---|---|---|
| **KnowBe4** | United States | Provision of Phishing Platform; Training Content; |