Terms and Conditions

Phishing Simulation & Awareness - Schedule CS-8

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary
Service Provider shall provide Phishing Simulation services to test and improve Client end-user awareness of phishing threats. Phishing Simulation services deliver controlled, simulated phishing emails to designated users to measure response rates, identify at-risk individuals, and support ongoing security awareness training. This service is intended to reduce risk by improving user behavior but does not guarantee prevention of phishing-related incidents.

Scope of Services
- Deployment of simulated phishing campaigns to Covered Users at agreed intervals.
- Customization of campaign difficulty, content themes, and delivery timing where supported by the simulation platform.
- Tracking and reporting of user responses, including open rates, link clicks, and credential submissions.
- Identification of high-risk users and targeted recommendations for remediation or additional training.
- Integration with Service Provider's security awareness training program where applicable.

Exclusions
- Guarantee that all phishing attempts will be prevented or that trained users will never fall victim to real-world phishing.
- Responsibility for disciplinary or HR actions related to user behavior or repeated failures in simulations.
- Creation of custom phishing content outside the capabilities of the standard platform (unless separately scoped).
- Support for users, applications, or mail systems not covered by Service Provider's simulation platform.
- Remediation of actual phishing or compromise incidents (covered under other security Schedules).

Client Responsibilities
- Authorize the use of simulated phishing emails within Client's environment, including whitelisting simulation domains as necessary.
- Inform employees, as appropriate, that ongoing phishing testing is a condition of employment or organizational security policy.
- Review simulation reports provided by Service Provider and take appropriate organizational action (e.g., retraining or policy reinforcement) for high-risk users.
- Ensure user cooperation with follow-up training where required.

General Terms
- Phishing Simulation is provided as a behavioral risk-reduction tool. While it improves awareness and preparedness, it cannot guarantee prevention of all phishing incidents. Even the most advanced training and testing programs remain subject to bypass or failure.
- Client acknowledges that Phishing Simulation is one element of a layered security strategy. Service Provider strongly recommends implementing complementary safeguards — such as endpoint detection and response (e.g., Adlumin XDR), multi-factor authentication, conditional access policies in Microsoft 365/Intune/Entra ID, DNS filtering, email security filtering, and ongoing defense training — to achieve stronger overall resilience.
- All response times for simulation-related service requests are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider's standard service fees unless otherwise specified. Additional costs (e.g., advanced custom campaigns or non-standard integrations) may apply and will be billed separately.