

Defense Training - Schedule CS-7

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

Service Summary

Service Provider shall provide Defense Training services (“Defense Training”) to educate Client’s end-users on security best practices, phishing awareness, and safe technology usage. The goal of Defense Training is to reduce human-factor risk by improving user awareness and response to threats. Training enhances Client’s overall security posture but does not guarantee that all users will recognize or avoid malicious activity.

Scope of Services

- Enrollment of designated Client end-users into a security awareness training platform.
- Delivery of online training modules covering topics such as phishing awareness, password hygiene, and safe data handling.
- Periodic refresher courses and new module assignments as available through the training platform.
- Tracking and reporting of user participation, completion, and test results.
- Access for Client management to review completion metrics and training progress.

Exclusions

- Responsibility for user actions or errors during day-to-day operations.
- Guarantee that training will prevent all security incidents or eliminate phishing success rates.
- Customized training content beyond the standard platform modules (unless separately scoped).
- In-person training sessions unless expressly agreed in writing.
- Support for non-enrolled users or contractors outside of the agreed training population.

Client Responsibilities

- Ensure designated end-users enroll in and complete assigned training modules.
- Promote training as part of organizational policy and enforce compliance among staff.
- Review training participation and completion metrics provided by Service Provider.
- Take corrective action for users who fail to complete training or demonstrate repeated high-risk behavior.

General Terms

- Dark Web Monitoring is a detection and notification service only; it does not prevent credential compromise.
- Client acknowledges that this Service is one element of a layered security strategy. While monitoring reduces risk by providing visibility into exposed credentials, no single control or combination of controls can guarantee complete protection or eliminate all vulnerabilities. Even the most advanced systems remain subject to bypass or compromise. 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, email filtering, DNS filtering, and security awareness training – to achieve stronger overall resilience.
- All response times for dark web-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. Vendor pass-through costs (e.g., licensing for dark web feeds or third-party platforms) may apply and will be billed separately.