Solutions Terms: Managed Security Awareness

Last Updated: May 2023

These Managed Security Awareness – Solution Terms describe the Managed Security Awareness Solution (the "Solution"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "Solutions Agreement") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). The Solution, if purchased by Customer via the Arctic Wolf website, will be provided in accordance with the terms located at https://arcticwolf.com/terms/ ("Website Terms"). The Solutions Agreement and Website Terms are collectively referred to herein as the "Agreement". Any capitalized terms not otherwise defined herein shall have the meaning set forth in the applicable Agreement.

Solution. The Solution provides Customers with an Administrator Dashboard and Content. The Content addresses current threat concepts to provide training and assist Users in the identification and prevention of system attacks within Customer's environment. The administrator dashboard (the "Administrator Dashboard") is an online, cloud-based learning management tool that allows Customers to manage its security awareness training activities and provides Customer with appropriate metrics, features, and functionalities to manage the security awareness activities of its Users.

Specific features and services provided as part of the Solution include:

Feature/Functionality:	**MA**	**MA+**
Microlearning awareness sessions that address deception tactics used, common red flags that should be recognized, escalation and response duties, and leadership responsibilities	Included	Included
Comprehension quizzes to track basic security posture and Customer's Users' comprehension of the Content	Included	Included
Managed phishing simulation built to represent threat vectors that Users are likely to encounter	Included	Included
Leaderboard point earning system for Users	Included	Included
Calculation of Customer's Secure Culture Score, as more fully described below	Included	Included
Alert issuance via the Administrator Dashboard	Included	Included
Access to reporting and account management	Included	Included
Advisory recommendations intended to improve Customer's culture of security	Included	Included
Dark web monitoring of Customer's domains	Included	Included
Access to licensed Content, including learning materials and additional resources contained in the Administrator Resource Library and/or Content Library within the Solution, by Customer and Users	Not included	Included
Arctic Wolf Report Email Button (O365 deployment required)	Included	Included
Reported Email Details, included in Phishtel Data, available for reporting within the Administrator Dashboard, including, date and time email reported, email address of reporting User, Microsoft Graph API ID	Included	Included
Reported Email Analytics which may be produced using Phishtel Data within the Arctic Wolf Phishtel Engine, including reported simulation details, analysis, and threat level, to aid in malicious email prioritization and management	Not included	Included
Content modifications ("SCORM") reasonably necessary to conform the Content to Customer's business format and standards, which shall be performed by Arctic Wolf, and are subject to the Arctic Wolf's Trademark usage requirements set forth in the Agreement and terms below	Optional Add-on for additional fees*	Optional Add-on for additional fees*
Ability to download certain Arctic Wolf designated Content from the Solution from an Arctic Wolf designated platform	Not included	Optional Add-on for additional fees*
Group-based Content assignment	Not included	Included
If licensed, access to Content Compliance Pack ("CCP"), an optional add-on module which includes compliance course content for common compliance topics that Administrators can assign to their users	Optional Add-on for additional fees*	Optional Add-on for additional fees*

Subject to an executed statement of work, custom professional and/or production services ("Custom Services")	Not included	Optional Add-on for additional fees*

*Feature and/or functionality is not available to Customer if license to Solution is purchased via the Website Terms.

Data Storage. Notwithstanding anything contrary in the Agreement or Order Form, as applicable, Customer's Confidential Information, as defined in the Agreement, is stored in Arctic Wolf's third-party service provider data centers located in the United States.

Tracking. Arctic Wolf will track participation rates, assessment scores, follow up completion rates, and phishing simulation click rates for Customer's users. This data will be used to calculate Customer's Secure Culture Score, as further described below, and identify remediation strategies for users.

Secure Culture Score. Customer's Secure Culture Score provided as part of the Solution is for illustrative and informational purposes only and may be used by Customer for internal benchmarking purposes. The Secure Culture Score is compiled using information related to Customer's and its users' participation in the Solution. Customer's Secure Culture Score is a live number that is calculated every time the Administrator Dashboard is loaded. Customer can download activity reports on demand through the Administrator Dashboard. Customer's Secure Culture Score will be available on Customer's online Administrator Dashboard.

Arctic Wolf Report Email Button. The Arctic Wolf Report Email Button, if deployed, provides Customer's Users the ability to self-report suspicious emails and automatically remove such reported email from a User's inbox. The Arctic Wolf Report Email Button is intended to provide Customer's Users with a tool to aid in a User's identification of suspicious emails. Customer's Administrators, through use of the Administrative Dashboard, and depending on the Solution deployed, may view certain available reports and analytics of the self-reported Phishtel Data.

SCORM. Subject to the additional qualifications herein and the applicable Agreement, Customer may request and purchase custom SCORM (SCO) modules. SCO modules include, but are not limited to, Arctic Wolf approved customizations such as (a) Customer specific branding, (b) Customer provided video assets, (c) reference or inclusion of Customer specific policies, action items, links, questions, quizzes, and other learning and development related requests, and (d) any available and required language subtitle files (.srt).

Custom Services. Subject to the additional qualifications herein and the applicable Agreement, Custom Services are any requests by Customer to change, edit, customize, or produce from scratch, existing or undeveloped Arctic Wolf Content, artifacts or deliverables, and/or any professional services or consulting. All Custom Services will be quoted and billed in accordance with an executed and agreed upon statement of work on a fixed fee basis.

Product Support. Customer can contact Arctic Wolf for assistance at security@arcticwolf.com or 888-272-8429 x2. Arctic Wolf will evaluate the request and collect related information from Customer. Customer is responsible for providing requested information to Arctic Wolf and implementing, in Customer's sole discretion, any remediation strategies identified by Arctic Wolf.

Customer shall have email access to the Arctic Wolf Support Center (in the location designated as the "Platform Location" on an Order Form, or in the case of a licensed purchased via the Website, in the United States) during standard support hours is available 8:00 am to 5:00 pm (based on the time zone within which the Support Center is located), Monday through Friday (excluding holidays). If Customer has more than one Solution login, Customer may appoint no more than five (5) contacts who are authorized to contact Arctic Wolf directly on behalf of Customer's Solution users.

Updates & Upgrades. Any automated maintenance and update cycles to the Solution will be performed remotely by Arctic Wolf.

Arctic Wolf may perform statistical analysis of the Solution and the Hosting Environment using Metrics Data. "Metric Data" means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) Customer provides to Arctic Wolf, or (ii) is collected or discovered during the course of Arctic Wolf's delivery of the Solutions or Customer's use thereof, excluding any such information or data that identifies Customer or to the extent that it includes personal information of Customer's data subjects.

Arctic Wolf Trademarks. Any license to Arctic Wolf Trademarks under the Agreement requires the following:

• All uses of Arctic Wolf Trademarks will comply with any written trademark guidelines that Arctic Wolf may provide to Customer from time to time.

• Customer is prohibited from removing or altering any Arctic Wolf Trademarks displayed with or in the Content or Hosting Environment except with Arctic Wolf's written consent or as otherwise accommodated by Arctic Wolf as part of the Solutions.

• Customer agrees that it will not in any way suggest or imply by the use of Arctic Wolf Trademarks that Customer is affiliated with or endorsed or sponsored by Arctic Wolf.

Additional Terms. To the extent the Solutions Agreement does not include terms related to the licensing of the Solution or specific new features and functionalities that have been added since execution of a Solutions Agreement, Customer and Arctic Wolf agree that the following additional terms and conditions will apply to Arctic Wolf's delivery and Customer's use of the Solution and/or newly added components thereof:

Solutions. Customer may purchase, when set forth on an Order Form, and Arctic Wolf, together with its Affiliates, may provide the applicable Managed Security Awareness Solution (the "Solution", and is contemplated as a "Solution(s)" as defined in the Solutions Agreement). Any terms not otherwise defined herein will have the meaning set forth in the Solutions Agreement.

The MA/MA+ Solution will be comprised of the following components:

Software	Phishtel Reporting Engine and Arctic Wolf Report Email Button
Equipment	N/A
Content	Online access and download rights, if licensed by Customer, to learning content and Content Compliance Pack within the Administrator Dashboard and/or Content Library
Content Management Hosting Environment	Access to and use of a cloud-based learning management tool (the "Administrator Dashboard") and metrics related to the use of the Content by Customer's users
Services	Support, onboarding services, and Content modification services, all as described in the Solutions Terms
Professional Services	SCORM and/or Custom Services, if any and as agreed by the parties in accordance with the Agreement
Platform	N/A

License Grant. The Solution is provided on a subscription basis for the Subscription Term for the Fees set forth on the Order Form. Provided Customer is compliant with the terms of the Solutions Agreement, including payment of Fees, Arctic Wolf grants to Customer a limited, non-transferable, non-sublicensable, non-exclusive right and/or license during the Subscription Term, to:
(i) Install, use, and access the Software,
(ii) Obtain and use the Services in conjunction with Customer's use of the Solution,
(iii) Load Customer's users and associated information for delivery of Content and use of the Administrator Dashboard,
(iv) Access Administrator Dashboard, subject to the Privacy Notice,
(v) Use Arctic Wolf Trademarks included in the Content in accordance with the Solutions Terms, and
(vi) Distribute, display, transmit, and, if licensed by Customer, download certain Content in electronic format.
Customer may access and use the Solution, and any Documentation associated therewith, solely for its own internal business purposes and in accordance with the terms and conditions of the Solutions Agreement, associated Documentation, and any scope of use restrictions and license counts, including by server, user, or such other applicable licensing metric.

Restrictions, Responsibilities, and Prohibited Use. In addition to any terms set forth in the Solutions Agreement, Customer agrees not to, directly or indirectly: (i) remove or obscure any proprietary or other notice contained in the Solution, including on any Content, reports, or data printed from the Solution; (ii) unless Customer is an authorized MSP partner of Arctic Wolf, use the Solution in connection with a service bureau, service provider or like activity whereby Customer operates or uses the Solution for the benefit of any third party; or (iii) include material or information that is obscene, defamatory, libelous, slanderous, that violates any person's right of publicity, privacy or personality, or otherwise results in any tort, injury, damage or harm to any person.

Confidentiality. In addition to anything set forth in the Solutions Agreement, Confidential Information includes the following:

First name, last name, corporate email address, phone number, job title, address, and organization hierarchy (collectively, **"Point of Contact information"**); User setup details (User email, work title, and name), Solution metrics related to such Users, including your Users' learning status, training scores, and Phishing results associated with such Users' use of the Solution (collectively **"Learner Data"**); if the Arctic Wolf Report Email Button is deployed by Customer, information pertaining to phishing email(s) self-reported by a User and includes or may include name of User, email address of User, Microsoft Graph API ID, json web token, full content of email, and version data (collectively, **"Phishtel Data"**); and Customer created and owned content, if any.

Termination. In addition to any other obligations upon termination set forth in the Agreement, Customer agrees to cease all use of the Content, installed, downloaded, or otherwise, and permanently erase or destroy all copies of any Content in its possession or under its control.