Offer Description: Cisco Security Awareness

This Offer Description (the **"Offer Description"**) describes Cisco Security Awareness (the **"Cloud Service").** Your subscription is governed by this Offer Description and the Cisco Universal Cloud Agreement located at www.cisco.com/go/uca (or similar terms existing between you and Cisco) (the **"Agreement"**). Capitalized terms used in this Offer Description and/or the Order not otherwise defined herein have the meaning given to them in the Agreement.

Table of Contents

1. Offer Description

Cisco Security Awareness is designed to help promote and apply effective cybersecurity common sense by modifying end user behavior. It empowers employees to work smarter and safer. This cloud delivered subscription provides comprehensive simulation, training and reporting so employee progress can be continually monitored and tracked. Cisco Security Awareness helps your organization remain safe with engaging and relevant computer based content with various simulated attack methods.

2. Supplemental Terms and Conditions

2.1. Restrictions

You agree that You will not: (a) license, sublicense, rent, lease, transfer, assign, time-share or otherwise commercially exploit the Cloud Service; (b) use the Cloud Services to collect, transmit or process any material that is infringing, obscene, threatening, libelous, or otherwise unlawful or tortious, including material that is harmful to children or violates third party privacy rights; (c) access the Cloud Services for the purpose of building a similar or competitive product; or (d) copy, translate, create a derivative work of, reverse engineer, reverse assemble, disassemble, or decompile the Cloud Services or any part thereof or otherwise attempt to discover any source code or modify the Cloud Services.

2.2. Usage of Phishing Simulator

If Your purchase includes the Phishing Simulator, the following terms apply: (a) the Phishing Simulator does not store any information directly provided by users being subjected to simulated phishing attempts. The Phishing Simulator collects such information as the IP address of the user, browser type, operating system, etc., which can then be incorporated in the reports generated by the platform; (b) You agree to use the Phishing Simulator only in compliance with applicable laws, including intellectual property laws. For greater clarity, the You agree that, when operating the Phishing Simulator, You will only make use of third-party text, graphic or other protected content with the permission of its owner or pursuant to an exception existing under applicable law, such as fair use, fair dealing or other similar exceptions, that allows for the use of protected content for educational purposes; (c) You acknowledge that the Phishing Simulator can only be used for training purposes, with the objective of increasing the

awareness of users to phishing attacks; (d) You may only use the Phishing Simulator internally, with its employees, and at all times in compliance with its internal policies; (e) You may only use the Phishing Simulator to send electronic mail messages to addresses belonging to domains owned by You or under Your control.

3. Data Protection

Cisco's data protection obligations are set forth in the Agreement. Additionally, the Cisco Cisco Security Awareness Privacy Data Sheet(s) (available here) supplement the Cisco Privacy Statement and describe the Personal Data that Cisco collects and processes as part of the delivery of the Cloud Services.

4. Support & Maintenance

The Cloud Services include online support and phone support. Cisco will respond as set forth in the table below and may require information from you to resolve service issues. You agree to provide the information requested and understand that a delay in providing the information to Cisco may delay resolution and response time.

Online Support allows access for support and troubleshooting via online tools, email and web case submission only. No telephone access is provided. Case severity or escalation guidelines are not applicable. Cisco will respond to a submitted case no later than the next business day during standard business hours.

Phone Support provides Cisco Technical Assistance Center (TAC) access 24 hours per day, 7 days per week to assist by telephone, or web case submission and online tools with use and troubleshooting issues. Cisco will respond within one (1) hour for Severity 1 and 2 calls received. For Severity 3 and 4 calls, Cisco will respond no later than the next business day.

You will also have access to Cisco.com, which provides helpful technical and general information about Cisco products, as well as access to Cisco's on-line knowledge base and forums. Please note that access restrictions identified by Cisco from time to time may apply.

The below table outlines Cisco's response objectives based on case severity. Cisco may adjust assigned case severity to align with the Severity definitions below.

Software Support Service	Technical Support Coverage	Response Time Objective for Case Severity 1 or 2	Response Time Objective for Case Severity 3 or 4
Basic with Phone Support	24x7 via Phone & Web	Response within 1 hour	Response within next Business Day
Basic with Online Support	Web	Response to all cases within next Business Day during Standard Business Hours	

The following definitions apply to this Section.

Response time means the time between case submission in the case management system to support engineer contact.

Severity 1 means the Cloud Service is unavailable or down or there is a critical impact to a significant impact to Case Submitter's business operation. Case Submitter and Cisco both will commit full-time resources to resolve the situation.

Severity 2 means the Cloud Service is degraded or significant aspects of Case Submitter's business operation are negatively impacted by unacceptable software performance. Case Submitter and Cisco both will commit full-time resources during Standard Business Hours to resolve the situation.

Severity 3 means the Cloud Service is impaired, although most business operations remain functional. Case Submitter and Cisco both are willing to commit resources during Standard Business Hours to resolve the situation.

Severity 4 means minor intermittent functionality or performance issue, or information is required on the Cloud Service. There is little or no impact to Case Submitter's business operation. Case Submitter and Cisco both are willing to provide resources during Standard Business Hours to provide assistance or information as requested.

Business Day means the generally accepted days of operation per week within the relevant region where the Cloud Services will be performed, excluding local holidays as observed by Cisco.

Local Time means Central European Time for support provided in Europe, Middle East and Africa, Australia's Eastern Standard Time for support provided in Australia, Japan's Standard Time for support provided in Japan and Pacific Standard Time for support provided in all other locations.

Standard Business Hours means 8am to 5pm Local Time at the location of the respective Cisco TAC, on Business Days, for the handling of TAC calls.

Your access to and use of the Cloud Services may be suspended for the duration of unanticipated or unscheduled downtime, including as a result of catastrophic events, external denial of service or other security breach, or operational incidents.

5. Service Level Objective

Cisco shall used commercially reasonable efforts to make the Cloud Services available at least 99.9% of each calendar quarter ("**Availability Target**"), except as provided below. Availability will be calculated per calendar quarter, as follows:

Availability = (X/Y) x 100, where:

X = the Total number of minutes of Service Availability, and

Y = (the Total number of minutes in the quarter) – (the Total # of minutes of downtime)

Definitions

Downtime means downtime that is not Excluded.

Excluded means (1) any planned downtime; Cisco will use commercially reasonable efforts to schedule all planned downtime during 5PM to 8AM on Saturdays (in the relevant data center's time zone) and (2) any unavailability caused by a problem by a Force Majeure Event.

Phishing Simulator means the platform that can help evaluate user awareness and maturity levels when handling phishing messages, and train users according to their specific roles and tasks.It supports building courses and quizzes, designing and launching phishing simulations, email management, analytics, user management, and much more.

Total means the total number of minutes in the calendar quarter minus the number of minutes of Excluded downtime during such quarter.