CYBER SECURITY – SERVICE DESCRIPTION

Managed Security Service Edge Services ("MSSE")

This Service Description ("**MSSE Service Description**") contains the terms governing the provision of Managed Security Service Edge services by Interactive Pty Ltd (ABN: 17 088 952 023) of 461 Williamstown Road, Port Melbourne VIC 3207 ("**Interactive**") to the customer named in the CMS SOW that applies to this MSSE Service Description ("**Customer**").

This MSSE Service Description forms part of the Agreement, also containing the Cyber Security Service Terms (found at www.interactive.com.au/terms-and-conditions) and the Master Services Agreement.

1 Managed Security Service Edge (MSSE)

1.1 Interactive will provide the MSSE Services for the Individual Term. The MSSE Services provide a cloud delivered service that leverages Netskope's technology to review and protect Customer web traffic at User and endpoint levels.

1.2 If the CMS SOW states that the Customer has purchased Security Service Edge (SSE) Next Gen Secure Web Gateway and Inline CASB, Interactive will provide the following:

(a) URL filtering capability.

(b) Threat and web traffic exploit protection capability with anti-malware engines.

(c) Data Loss Prevention capability for cloud apps, web services and web traffic.

(d) Infrastructure as a Service ("**IaaS**") and Platform as a Service ("**PaaS**") User traffic monitoring capability.

(e) Capability to classify Cloud Apps with a risk score.

(f) Configuration of the policies set out in the Managed Alerts RACI table in CMS SOW.

1.3 If the CMS SOW states that the Customer has purchased Security Service Edge (SSE) with CASB API Protection, Interactive will provide the following:

(a) Detection capability of bulk delete, bulk downloads, and bulk uploads of sensitive data in monitored cloud applications.

(b) Detection capability of impossible travel Security Events.

(c) Detection capability of rare User activity and risky web activity.

(d) Configuration of the policies set out in the Managed Alerts RACI table in CMS SOW

1.4 If the CMS SOW states that the Customer has purchased Security Service Edge (SSE) with Private Access), Interactive will provide the following:

(a) Capability to publish applications that are in data centres or public cloud environments via a Publisher application gateway with a one-way outbound connection.

(b) Capability for a Cloud Agent to authenticate and authorise access to Customer resources (business internal applications, sanctioned cloud business applications, etc.)

2 Onboarding

2.1 As part of the onboarding process, Interactive and the Customer will agree on certain pre-approved actions that Interactive can perform in the event of a Security Incident.

2.2 The Customer authorises Interactive to deploy a Cloud Agent on the Devices (included in the scope of the MSSE Services) and acknowledges that the Cloud Agent being deployed on Devices can impact performance.

2.3 As part of the onboarding process Interactive and the Customer will agree on a plan detailing the activities required to be completed by the Customer and Interactive personnel to implement the MSSE Service contracted by the Customer.

2.4 On completion of the activities agreed pursuant to clause 2.3, Interactive will notify the Customer of the date the Customer may commence conducting Acceptance Tests ("Acceptance Test Commencement Date").

2.5 The Customer shall complete the Acceptance Testing no later than 5 Business Days of request.

2.6 If the Customer's Acceptance Testing identifies any defects caused by Interactive that prevent the Customer from receiving the tested Services, the Customer may provide Interactive with notice in writing rejecting the Acceptance Tests and detailing the reasons why. If the Customer delivers that notice:

(a) the parties shall work together to identify and correct the error that caused the Acceptance Tests to fail; and

(b) after the cause of error is corrected, Interactive will notify the Customer of a new Acceptance Test Commencement Date and, in that event.

2.7 If the Customer, acting reasonably, delivers more than two notices rejecting the results of the Acceptance Tests, either party may refer the matter for resolution in accordance with the dispute resolution provisions in the Master Services Agreement.

2.8 If the Customer fails to complete Acceptance Testing or delivers a notice rejecting the Acceptance Tests within 5 Business Days after the Acceptance Test Commencement Date, then Acceptance Testing will be deemed completed by the Customer. After all Services have completed Acceptance Testing, or are deemed to have completed Acceptance Testing, Interactive will provide the Customer with a notice informing it of the Service Start Date.

3 Customer Obligations

3.1 The Customer must ensure the following internet traffic (inbound and outbound) is permitted between all Customer endpoints (included in the scope of the MSSE Services) and the Netskope infrastructure.

(a) Internet IP addresses: 163.116.128.0/17 (Netskope cloud infrastructure) Port: TCP 443

(b) Internet IP addresses: 8.8.8.8 and 8.8.4.4 (Google DNS infrastructure) Port: TCP 53 & UDP 53

Further information about the network accessibility requirements is outlined in the following URL: https://docs.netskope.com/en/check-firewall-policy.html

3.2 The Customer must ensure that the network communications described in clause 3.1 are permitted through all firewalls controlling the traffic between the endpoints (included in the scope of the MSSE Services) and the internet.

3.3 The MSSE Service relies on Cloud Agents and can therefore not be supported if the Cloud Platform Vendor has not certified the Cloud Agent on a specific Cloud Platform. The Customer must ensure that the Cloud Agent and/or MSSE sensor is supported and may view the latest list of support platforms at the following URLs (or successor URLs):

(a) Netskope: https://docs.netskope.com/en/netskope-client-supported-os-and-platform.html

4 Reporting

4.1 Interactive will provide a standard monthly service report to the Customer.

4.2 During the onboarding process the Customer will be provided with the standard monthly service report template.

5 MSSE Services Pricing

5.1 The Service Fees for the MSSE Services are based on the quantity of Devices and the type of the MSSE Service purchased by the Customer. The different types of MSSE Services are described in clauses 1.2, 1.3 and 1.4 in this Service Description.

5.2 The Customer may request to add Devices by making a Service Request and providing relevant details. Interactive will add the Devices, and the Customer will be charged for the addition pro-rata from the date the Device is added, and the calculated amount will be included in the monthly bill in arrears.

6 Support and Response

6.1 Interactive will provide level 1 support for management of issues related to the MSSE's configured policies, initial network issues triage and issues related to Interactive managed infrastructure. Interactive may require the Customer's technical SMEs to make themselves available to provide support with any issue being reviewed. For anything above basic MSSE's policy support; the Customer's internal IT teams or Customer's technology service providers will need to make themselves available to work on level 2 and above issues.

Incident Priority Matrix	**Impact**				
	Extensive / Widespread		**Significant / Large**	**Moderate / Limited**	**Minor / Localized**
Urgency	**Critical**	P1	P1	P2	P3
	High	P2	P2	P3	P4
	Medium	P3	P3	P4	P4
	Low	P4	P4	P4	P5

SLA (indicative)	
Priority	**Response**
P1	0.5 hours
P2	1.5 hours
P3	4 hours
P4	8 hours
P5	16 hours

7 Exclusions

7.1 The MSSE Services do not include any of the following:

(a) Deployment of Publishers and administration of infrastructure for management of Publishers.

(b) Deployment and management of Software Defined Networks (SD-WAN).

(c) Advanced troubleshooting of infrastructure issues, or Advanced Issues the Customer may encounter.

(d) Protection of "Private Applications" will not be enabled as this capability will require a specific license not included in the service.

(e) Utilisation of additional features like Cloud Firewall will, if required, be charged at time and materials rates.

(f) Deployment of virtual appliances, if required, will be charged at time and material.

8 Definitions

8.1 The following definitions apply to this MSSE Service Description:

Advanced Issues refers to operational issues that require intervention of Netskope to be solved like zero-day vulnerabilities. Or issues related to technology components outside the scope of the service being provided like problems at operating system level on endpoints for example.

Cloud Access Security Broker (CASB) is a visibility and control point that secures cloud applications, delivering data protection and Threat Protection services to prevent leakage of sensitive data, stop malware and other threats, discover and control shadow IT, and ensure compliance. Sitting between cloud app Users and cloud services, CASBs can monitor traffic and User activity, automatically block threats and risky sharing, and enforce security policies such as authentication and alerting.

Cloud Agents means software agents that steer traffic from end User devices to the Cloud Platform for securing User and endpoint traffic. The Netskope Cloud Platform utilises Netskope Clients.

Cloud Platform refers to the distributed platform used by the MSSE Service to conduct cloud security event management.

Cloud Platform Vendor means the person or entity providing the Cloud Platform, which may a third party engaged by Interactive.

Data Loss Prevention is a security solution that identifies and helps prevent unsafe or inappropriate sharing, transfer, or use of sensitive data to assist the Customer to monitor and protect sensitive information across on-premises systems, cloud-based locations, and endpoint devices.

Device(s) is a laptop, workstation or a server that supports the installation of the Netskope client-side software.

MSSE Services means a cloud-based service that provides malware protection, URL filtering and threat prevention and incorporates Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) and a Secure Web Gateway (SWG).

Private Applications are internal applications (hosted on on-prem data centres or private data centres) that Users will be able to access remotely.

Publisher – A piece of software that is part of a Private Access Gateway that delivers application authentication and authorisation to the Cloud Agent.

Security Event means a condition or situation detected by the Cloud Platform, which is observed from one or more Cloud Agents.

Security Incident means one or more Security Events identified by the Customer or Interactive to be an adverse condition or situation in the IT Environment.

Threat Protection is the cyclical practice of planning, collecting, processing, analysing, and disseminating information that poses a threat to applications and systems.

User means an employee, contractor, or any other authorised person utilising customer systems.

Zero Trust Network Access is a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack.