Managed SASE Services - Service Terms

These **Services Terms** (“**Terms**”) contain the terms governing the provision of the Managed SASE Services (“**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 (“**Customer**”). The Master Services Agreement applies to these Terms and the CMS SOW.

1 Services

1.1. Interactive will provide the Managed SASE Services to the Customer that are specified in the CMS SOW.

1.2. The Platform Management Services described in clause 14 are essential and apply to all Managed SASE Services set out in clause 1.3.

1.3. The Service Descriptions for each of the Managed SASE Services are detailed in these Terms as follows:

(a) Service Description - SASE Network Operations Centre (NOC Level 1) is set out as clause 15.

(b) Service Description - SASE Incident Management is set out at clause 16

(c) Service Description - SASE Identity Integration is set out at clause 17.

(d) Service Description - SASE SD-WAN Integration is set out at clause 18.

(e) Service Description - SASE Policy Configuration and Management is set out at clause 19.

(f) Service Description - SASE Cloud Delivered Security Services Standard is set out at clause 20.1

(g) Service Description - SASE Cloud Delivered Security Services Advanced is set out at clause 20.2.

2 Term of Services

2.1 Interactive will provide the Services for the Individual Term.

2.2 Subject to clause 2.3, for planning and pricing and ensuring continuity of service purposes and unless otherwise detailed in the CMS SOW or otherwise agreed in writing:

(a) not less than 30 days before the end of the Service Term or a current Further Term of a CMS SOW either party may serve written notice on the other party stating it will not renew the CMS SOW; and

(b) if no such notices are served under clause 2.2(a), each CMS SOW renews for successive terms of the lesser of (i) the original contract term; or (ii) 12 months (each successive term being a “Further Term”), at the end of its Service Term and each Further Term.

2.3 If the Customer is a consumer or small business (as defined by the *Competition and Consumer Act 2010* or the *ASIC Act 2001*):

(a) the Customer may serve written notice to terminate a CMS SOW within no less than 30 days at any time after the end of the original Service Term or at any time during a Further Term of a CMS SOW; unless

(b) not less than 60 days before the end of the Service Term or a current Further Term of a CMS SOW, Interactive had sent a written notice to the Customer reminding them of the upcoming renewal.

3 Solution Description

3.1 The Services will be delivered to the specifications detailed in the CMS SOW and applicable Service Description, unless otherwise agreed by the parties in writing during Project delivery.

4 Pricing Terms

4.1 The monthly Service Fees for Managed SASE Services are payable by the Customer from the Service Start Date. Interactive will issue invoices to the Customer for the Managed SASE Services in advance.

4.2 The monthly Service Fee for Managed SASE Services comprises;

(a) a Platform Management Fee per Environment for all Tiers of Services; and

(b) a per User Fee for each of the Standard and Advanced Tiers of Service which is calculated by multiplying the Unit Price by the volume of Users under management in the month.

4.3 Interactive may adjust the monthly Service Fee annually for each of the Services detailed in the CMS SOW (for the avoidance of doubt, this change applies to both initial and additional Services) by giving no less than 30 days' notice to the Customer.

4.4 Interactive may vary the monthly Service Fee when a variation to the Services is necessary due to Changes in the Customer's volumes, and this shall occur as either an addendum to the CMS SOW or in accordance with the Change Management Process.

4.5 The Managed SASE Services set out in the CMS SOW are the estimated Solution and indicative monthly Service Fee and are based on the information the Customer has provided to Interactive as at the date of the CMS SOW. The Customer agrees and acknowledges the Managed SASE Services provided by Interactive may be varied based on information obtained during the Onboarding Stage.

4.6 All pricing is exclusive of GST. GST will be charged in addition.

4.7 With respect to any Third-Party Software, if the relevant Third-Party Software Vendor:

(a) increases its licence fees or introduces new licence fees for their products that directly relate to the Managed SASE Services being provided to the Customer, Interactive may increase the Service Fees upon 30 days' written notice from Interactive to the Customer; or

(b) issues a billing correction to Interactive that directly relates to the Managed SASE Services, Interactive may issue an additional invoice to the Customer in respect of the billing correction, which may include retrospective Service Fees payable.

5 Service Calls

5.1 Interactive will provide the Customer the ability to log a Service Call via the Service Desk to report an Incident or make a Service Request.

5.2 The Customer must make a Service Call as follows:

(a) Phone: 1300 669 670 (in Australia) or +61 2 9200 2679 (internationally); or Customer dedicated 1300.

(b) Email: cmssupport@interactive.com.au ; or

(c) By contacting the Account Executive or Service Delivery Manager assigned to the Customer.

6 Service Request

6.1 A Service Request may be logged by the Customer, or Interactive on the Customer's behalf.

6.2 A Simple Service Request is a request from the Customer for a simple move or change to the contracted Services, determined by the Interactive to be a request that:

(a) is non-complex and does not require planning or due diligence;

(b) can be completed in 4 hours or less, by a single engineer and during Business Hours; and

(c) does not require representation at Interactive's change advisory board.

6.3 If the Customer makes a request that is not a Simple Service Request, or requires planning, due diligence, multiple engineers or will take more than 4 hours to complete, Interactive will treat these requests as a standalone project ("**Billable Service Request**"). Interactive will provide estimated delivery timelines for Billable Service Requests as part of the project plan, which is developed in consultation with the Customer during the project. Interactive cannot guarantee project delivery timelines for requests as timelines vary depending on the complexity of the change and the availability of each party's Personnel.

6.4 The following applies to the Services listed in the tables at clause13.2:

(a) **Simple Service Request:** If a Service is indicated to be available via Simple Service Request:

(i) Interactive will execute up to the maximum number of Simple Service Request Entitlements per month as defined in the CMS SOW subject to the following provisions.

(ii) Where the Customer consumes more that the Simple Service Request Entitlement, Interactive will enact the Fair Use Policy described in clause 6.5 and may require the Customer to purchase additional bundles of Simple Service Requests.

(iii) The Simple Service Request Entitlement count will be reset at the end of every quarter, which means any underutilised Simple Service Requests cannot be rolled over to next quarter.

(iv) The Customer may increase the Simple Service Request Entitlement by purchasing additional Simple Service Request bundles.

(v) The following Services are excluded from the scope of Simple Service Requests; and if required may be requested with a price on application (POA):

A. Custom development (e.g., scripts, integrations).

B. Training or enablement.

C. Application-level support (unless specified).

D. Vendor liaison outside of network and security platforms.

(b) **Billable Service Request:** If a Service is indicated to be available via Billable Service Request, Interactive will perform the Services upon request for an additional fee, as they are not covered by the monthly Service Fees. Charges for Complex Service Requests are based on price on application (POA).

6.5 **Fair Use Policy:** The Customer must abide with the Fair Use Policy applicable to monthly Simple Service Request Entitlements defined by Interactive below:

(a) **Purpose:** This policy is designed to prevent excessive, repetitive, or automated use of Service Requests that may degrade service quality or lead to unfair usage patterns.

(b) **Fair Use Limits:** The Customer is expected to submit Service Requests in a manner aligned with the size and complexity of their managed environment.

(i) Repeated submission of similar or low-effort requests (e.g., multiple password resets, minor configuration changes) may be flagged for review.

(ii) The following thresholds may trigger a usage review:

A. Submitting more than the monthly entitlement consistently for 2 or more months.

B. Submitting more than 3 times the monthly entitlement in a given month.

C. Logging 5 or more Service Requests in a 24-hour period without clear justification.

D. Submitting multiple redundant requests for the same issue or change.

(c) **Usage Review & Action:** If the Customers request volume significantly exceeds the Simple Service Request Entitlement set out in the CMS SOW, Interactive may:

(i) Initiate a usage review and provide a report of request patterns.

(ii) Recommend adjustments to operational processes (e.g., automation or self-service options).

(iii) Suggest a higher support tier or the purchase of additional Service Request bundles.

(iv) In extreme or sustained cases, limit non-critical Service Request processing until a resolution is agreed upon.

(d) **Encouraged Practices:** To manage request volumes efficiently, Interactive encourages Customers to:

(i) Consolidate related Service Requests into single tickets where appropriate.

(ii) Use available self-service or automation tools (e.g., portal actions, scripts).

(iii) Prioritise critical issues when nearing entitlement limits.

7 Project Delivery

7.1 Each party will assign a Project Manager and confirm an expected Project start date.

7.2 If the Customer is delaying the Project, Interactive may send the Customer a notice requiring it to rectify the delay within five (5) Business Days. If the Customer fails to or is unable to rectify the delay, Interactive may complete the remaining activities that are not dependent on the Customer and issue a notice confirming the Service Start Date (for the avoidance of doubt in these circumstances the provision of this notice will not require any Acceptance Tests to have occurred).

Due Diligence

7.3 The parties shall conduct the Due Diligence stage to confirm the accuracy of the information the Customer has provided to Interactive and identify any possible issues or impact upon the Project.

7.4 If any issues are identified by Interactive which affect the Solution, the parties may agree to change the Solution in accordance with the Change Management Process (clause 8) or the Assumptions (clause 11).

Customer Onboarding

7.5 During the Onboarding Stage, Interactive will liaise with the Customer to develop a project plan and project schedule and complete the installation of the ongoing management toolset and agree the scope of each Service.

7.6 Interactive will perform the Onboarding Stage in accordance with the agreed project plan and the activities set out in clause 21.

Acceptance Testing

7.7 On completion of the Onboarding Stage for each Service, Interactive will notify the Customer of the date the Customer may commence conducting Acceptance Tests (“Acceptance Test Commencement Date”).

7.8 The Customer shall complete Acceptance Testing no later than five (5) Business Days after the Acceptance Test Commencement Date.

7.9 If the Customer’s Acceptance Testing identifies any defects caused by Interactive that prevent the Customer from using 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, clause 7.7 will apply again.

7.10 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.

7.11 If the Customer fails to complete Acceptance Testing or deliver 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.

8 Change Management

Prior To The Service Start Date

8.1 Before the Service Start Date, if either party requests any change to the CMS SOW, that party shall submit to the other party a Project Change Request (“PCR”).

8.2 The party submitting the PCR shall describe the change, the rationale for the change and Interactive will advise on the effect the change will have on the Services and relevant fees in the PCR.

8.3 Each party's Project Manager shall review the proposed change and may then either approve it, submit it for further investigation or reject it.

8.4 If both parties agree to the PCR, they shall sign the PCR and, from the date it is signed, the CMS SOW will be amended according to the changes described in the PCR. If the PCR is not agreed to, the CMS SOW will continue to apply unchanged.

After The Service Start Date

8.5 After the Service Start Date, if the Customer requests changes to the Services, the Customer may make a request for the changes as follows:

(a) If the Customer requests changes to items that are listed in the Service Catalogue, Interactive shall provide the changes requested, subject to the limits specified in the Service Catalogue, and the Customer shall pay Interactive the Service Fee set out in the Service Catalogue effective upon activation of the Service item.

(b) If the new services are not available in the Service Catalogue, Interactive will consult with the Customer to identify a solution, including how to implement it, and provide a quotation for the new services. If the Customer accepts the quotation in writing, Interactive shall provide those new services as set out in the quotation and the Customer shall pay Interactive the fee set out in the quotation.

9 Licensing

9.1 Unless specifically detailed in the CMS SOW that Interactive provides licencing, the following applies:

(a) The Customer shall have appropriate software licensing for all Managed SASE Services and Devices under support scope.

(b) The Customer shall obtain valid licenses and obtain software maintenance services for its hardware and software, including upgrades necessary to correct defects. To the extent that the Customer is a party to a software agreement under which a third party provides software maintenance for its software, the Customer will make the benefits of such maintenance available to Interactive to enable Interactive to perform the Services.

(c) The Customer warrants it has procured the required licences and rights of use for all software the Customer relies upon for business functionality. The Customer shall pay all costs incurred in complying with this clause, unless otherwise agreed in writing by the parties.

(d) The Customer warrants that it is responsible for obtaining and complying with all necessary software licences and vendor support agreements for their hardware, software and their associated costs and the Customer indemnifies Interactive with respect to same without limitation.

9.2 Except for guarantees that cannot be excluded by law, Interactive expressly disclaims all guarantees and warranties, whether express, implied or otherwise, including without limitation, guarantees of merchantability, quality and fitness for a particular purpose in respect of the Third-Party Software. Interactive does not guarantee or warrant that the Third-Party Software will be available, uninterrupted or error free, meet the Customer's requirements, or operate with the combination of hardware and software the Customer intends to use, including Services provided by Interactive.

10 General Customer Responsibilities

10.1 During the Onboarding Stage the Customer shall:

(a) Define initial security policies and business requirements for SASE;

(b) Provide policy rules, access control lists that are to be configured in the SASE solution;

(c) Approve baseline configurations or adjust them in the portal;

(d) Ensure policies align with corporate standards (e.g. acceptable use, segmentation) before go-live;

(e) Designate Customer Incident contacts and escalation paths;

(f) Set communication protocols and include Interactive in internal Incident Response procedures;

(g) Provide network underlay/connectivity or information for each Customer site location; and

(h) Review connection of identity sources (SSO/AD) and ensure environment (power, cabling) is ready for any SASE hardware.

10.2 During the Service Term the Customer shall:

(a) Continuously oversee and review Interactive’s deployed policies and promptly notify Interactive of any required changes;

(b) Regularly assess policy effectiveness and Initiate policy changes via change requests or self-service for new apps, threats, or compliance updates;

(c) Participate in bridge calls related to the Managed SASE offering hosted by Interactive during Major Incidents;

(d) Coordinate with Interactive on containment and recovery;

(e) Raise Service Requests to add new Users/locations into SASE;

(f) Notify Interactive of infrastructure changes that impact the service;

(g) Ensure ongoing adherence to laws. The Customer remains responsible for legal compliance in use of the service;

(h) Inspect audit evidence (logs, reports) that are collected from Interactive;

(i) Include SASE in annual security reviews and third-party audits;

(j) Ensure the SASE setup meets all compliance requirements;

(k) Specify any data residency or encryption needs;

(l) Obtain any necessary User consents for traffic monitoring;

(m) Document the SASE system in security policies and risk assessments;

(n) Notify Interactive of any planned changes to relevant network segments (such as changing an ISP, renumbering IP addresses, etc.);

(o) Notify Interactive on opening of new branch offices or remote Users joining the company;

(p) Maintain any on-site devices or infrastructure under Customer care;

(q) Upon notification from Interactive, the Customer must investigate impacts inside its environment if an Incident is detected. For example, this could occur during a malware outbreak, unauthorized access attempt, network outage or any other unprecedented issue; and

(r) Reviewing compliance reports/certifications.

11 Assumptions

11.1 Interactive relies on the information provided to it by the Customer to be able to perform the Services as required by this Agreement. If any assumptions made by Interactive made or set out in the CMS SOW are proven to be incorrect including because the information provided by the Customer was incorrect or inadequate, or if the technical requirements are proven to be beyond the capability of the Solution, Interactive will negotiate with the Customer with respect to one of more of the following:

(a) altering the Solution which may require a change in accordance with the Change Management Process,

(b) adjust the project schedule in relation to any changes required to the solution; and

(c) adjust either or both the implementation fee and the monthly fees as a result of the alterations to the project.

11.2 The following assumptions apply:

(a) Interactive is reliant on the Service Level Agreements the Customer has in place with its existing vendors when a Device/part failure has occurred, any new spare part must be supplied by the original equipment manufacturer.

(b) All software and firmware on in-scope Devices and systems are current and on the supported version at the Onboarding Stage.

(c) Onboarding Stage requirements are met, including but not limited to that the Customers environment is compatible with Interactive's management and monitoring tools and utilities.

11.3 Data transfer entitlements per User are determined by the SASE vendor and apply to each Customer tenant. The Customer may make annual pre-purchases of additional entitlements. Any usage beyond the purchased amount will incur additional charges.

11.4 The Customer will manage any Endpoint Security Service, such as EDR or MDR, unless they have purchased such service separately from Interactive under a Statement of Work.

11.5 Interactive will provide the SASE agent installation package for deployment on each User's device. The Customer may deploy the agents themselves unless they have purchased the Managed End User Device Service from Interactive, in which case Interactive will perform the deployment.

12 General Exclusions

12.1 The following items are Out of Scope and are not included in the Services provided by Interactive unless specifically detailed in the CMS SOW, but may be available by agreement in writing between the parties in accordance with the Change Management Process and will be charged in accordance with the Standard Charge Out Rate:

(a) Anything not listed as being in-scope as part of the Services is excluded.

(b) Ongoing Network Management (LAN/WAN).

(c) Agent deployment of Security Services Edge (SSE) is managed by the Customer, unless the Customer has purchased Interactive's Managed End User Device Service.

(d) Any hardware and software version upgrades are excluded as part of the monthly service unless specified in the Service Description. The upgraded scope will be defined and performed as a project on a time and material basis.

(e) Any hardware or software that is not licensed or has no support agreement in place.

(f) Service Levels for out of support / end of life Devices are excluded. Any Devices, systems or software that are end of life or end of support (not supported by the vendor and/or no patches or updates being developed) or is not an in-scope service can be managed and supported on a best-efforts basis at an additional charge. If there are any issues with these Devices, systems or software, Interactive will attempt to fix the issue however, it is not responsible, and no Service Level Agreement (SLA) is applicable.

(g) Remediation of any defects found on the Devices during the Onboarding Stage including updating any firmware to a current version.

(h) Hardware maintenance, unless the Customer has entered into an agreement with Interactive to provide such services.

(i) Communications links, unless the Customer has entered into an agreement with Interactive to provide such services,

(j) Installation of application software and third-party software patches.

(k) Provide Customer with relevant information for auditors.

(l) Cyber Services such as MDR, unless the Customer has purchased the relevant services separately from Interactive under a relevant Statement of Work.

(m) End User Support is the Customer's responsibility unless Managed End User Device Support is purchased from Interactive as part of Interactive's Digital Workplace Services.

Application package installation is the Customer's responsibility unless purchased through Interactive's Digital Workplace Services.

12.2 If Interactive provided the Customer with recommendations to rectify or mitigate issues within the Customer's environment and the Customer did not implement the recommendations, and those issues caused or contributed to loss or liability being incurred by the Customer, the Customer irrevocably releases Interactive from and indemnifies Interactive against any loss or liability.

13 Managed SASE Service Tiers

13.1 The Platform Management Tier is included in all service engagements, while the Standard and Advanced Tiers are available as optional upgrades based on Customer selection as detailed in the CMS SOW.

13.2 The following table details the relevant inclusions in each Tier of Service as further described in these Service Terms:

Services / Service Details	**Service Tier**		
	Platform	**Standard**	**Advanced**
SASE Platform Management: - Monitoring only - No incident / no break fix - Health Reporting - Guidance only for SASE polices (up to 2 service calls per month), no policy changes	✓	✓	✓
SASE Network Operations Center (NOC level 1)	x	✓	✓

SASE Incident Management	x	✓	✓
SASE SD-WAN Integration	x	✓	✓
SASE Policy Configurations and Changes	x	✓	✓
SASE Identity Integration	x	✓ Single IdP only	✓ Multiple IdPs
Cloud Delivered Security Service - Standard	X	✓Up to 5 policies	x
Cloud Delivered Security Service - Advanced	X	x	✓ Greater than 5 Policies
Service Request Entitlement	x	✓Up to 5	✓ Up to 10

14 Service Description – SASE Platform Management

14.1 The SASE Platform Management Services include the following:

(a) **Managed Monitoring:**

(i) Interactive will provide monitoring for in-scope services within the Customer's Environment. This monitoring will include monitoring of the network and security posture of the Customer's environment such as network performance.

(ii) Interactive will leverage the available functionality and services of the relevant SASE vendor to provide the Platform Services.

(b) **Stakeholder co-ordination:** Interactive will liaise with all relevant stakeholders including vendors and the Customer to co-ordinate the monitoring and triaging of alerts.

(c) **Centralised administration:** Interactive will provide a centralized read-only view of the SASE platform to the Customer, to enable the Customer to review security and network policies across the Customer tenancy.

(d) **Guidance:** Interactive will provide assistance to the Customer to align SASE policies, up to 2 Service Calls per month, in line with their business goals.

(e) **Health Reporting:** Interactive will provide standard and custom reporting as part of the CMS SOW:

(i) **Standard Reporting:** Interactive will provide a standard monthly service report to the Customer. This report will include standard information related to network and security posture of the Customer's SASE environment. Some examples include real-time visibility into network performance, SLA events, bandwidth usage, or, number of threats blocked. During the Onboarding Stage the Customer will be provided with the standard monthly service report template.

(ii) **Custom Reporting**: Interactive will collate any specific requirements of the Customer and build custom reports on a demand basis. This service will be provided at an additional charge in accordance with the Standard Charge Out Rate.

15 Service Description – SASE Network Operations Center (Level 1 NOC)

15.1 If the CMS SOW states that Interactive provides Network Operations Centre (Level 1 NOC_ Services, Interactive will provide NOC Services that provide a centralized, proactive management and support for network and security service.

15.2 The NOC Services include the following:

(a) Integration with Interactive's Service Desk for initial contact, triage and troubleshooting.

(b) Ongoing monitoring of Managed SASE Services.

(c) Escalation processes to Interactive's Managed Network Services and Hardware Maintenance Teams.

(d) Ensuring continuous service availability and rapid response to issues.

(e) Vendor coordination for support and escalations.

15.3 The NOC Services will exclude the following:

(a) Management and support for Devices.

(b) Activities related to third-party tooling, documentation, or ITSM toolsets that are not part of the standard offering.

(c) Ongoing projects, remediation, or modernization work in the environment that is not part of the standard offering.

16 Service Description – SASE Incident Management

16.1 If the CMS SOW states that Interactive provides SASE Incident Management Services Interactive shall perform the following activities:

(a) fix escalated Incidents beyond basic triage.

(b) perform in-depth troubleshooting of SASE issues, apply known fixes, and restore service where possible.

(c) identify issues and implement standard remediation for the identified issues.

(d) Communicate updates to the Customer (typically via ServiceNow ticket and email/phone for P1s).

(e) Lead the Incident resolution related to the SASE offering as Major Incident managers for P1s.

(f) Engage vendor support for bug fixes or cloud issues.

(g) Escalate to third parties if necessary.

(h) Ensure root cause analysis and permanent fix (PCA) are identified and documented post-Incident.

16.2 The following is excluded from the SASE Incident Management Service:

(a) Development of custom scripts, APIs, or integrations with third-party platforms.

(b) Regulatory or legal compliance support.

(c) Incident Response for Nation-State or Advanced Persistent Threat (APT) Attacks.

(d) Hardware replacement or onsite support.

(e) End-user training.

17 Service Description: SASE Identity Integration

17.1 If the CMS SOW states that Interactive provides SASE Identity Integration Services, Interactive shall perform the following activities:

(a) Interactive will leverage the SASE's SSO capabilities to authenticate Users via the Customer's IdP viz Entra ID, ensuring a unified identity across cloud and network access. Interactive will integrate the SASE solution with the Customer's chosen Identity Provider (IdP) so that the SASE trusts that IdP for authentication.

(b) Interactive will continuously monitor the endpoint posture (OS patch level, antivirus status etc.) and tag device compliance. Interactive will provide an end-to-end Zero Trust architecture for remote and distributed access, also authenticating Users through a strong SSO+MFA process.

(c) Interactive will provide identity-based policy enforcement. Role-based access rules ensure least privilege: e.g. only Finance group Users (with compliant devices) reach finance apps. All web and application traffic is governed by User-specific policies.

(d) Interactive will connect the SASE solution with single (Standard Tier) or multiple IdPs (Advanced Tier) that the Customer uses. This integration will offer federation, provisioning and MFA services during the Onboarding Stage and ongoing management as IdP configurations evolve.

(e) Interactive will provide ongoing identity lifecycle management. This includes managing the User identity through its life cycle: Onboarding new Users with the correct access, updating privileges as roles change, and promptly revoking access for departures or as soon as a threat is noted.

17.2 The following is excluded from the SASE Identity Integration Services:

(a) Identity solutions other than Entra (Azure AD).

(b) Ongoing administration and management of IdP.

18 Service Description: SASE SD-WAN Integration

18.1 If the CMS SOW states that Interactive provides SASE SD-WAN Integration Services, Interactive will Integrate the SASE solution with SASE SD-WAN or on-premises appliances.

18.2 As an example, SASE cloud points of presence (PoPs) interconnect with existing SD-WAN hubs, extending secure access to branch offices without complex new infrastructure.

19 Service Description: SASE Policy configuration and changes

19.1 If the CMS SOW states that Interactive provides SASE Policy Configuration and Change Services Interactive will provide the following:

(a) Perform deployment of changes to the configuration and policies using the Vendor's centralized management system. The number of changes is determined by the Tier of Service purchased by the Customer as set out in clause 13.

(b) The following is excluded from the SASE Policy Configuration and Change Services:

(i) Integration with other tools (e.g. Intune), which is the responsibility of the Customer, unless the Customer purchases this as part of the Digital Workplace Services.

20 Service Description: Cloud Delivered Security Services

20.1 **Standard Tier**

(a) If the CMS SOW states that the Customer has purchased the Cloud Delivered Security Services under the Standard Tier**,** Interactive will provide the following:

(i) Essentials Secure Web Gateway (SWG) and Inline Cloud Access Secure Broker (CASB):

A. Web Security Policy (URL filtering capability, category controls).

B. Threat and web traffic exploit protection capability with anti-malware engines.

C. Basic 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. Restrict tenant access to SaaS applications using SASE Web Filter with Inline-CASB and SSL deep inspection.

F. Allow, monitor, or block SaaS traffic access using SASE Application Control with Inline-CASB and SSL deep inspection.

G. Configuration of policies in agreement with the Customer.

(ii) Essentials CASB API Protection:

A. API integration for sanctioned SaaS (O365, GDrive, Box), visibility into file sharing and external collaboration.

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

C. Detection capability of impossible travel security events.

D. Detection capability of rate User activity and risky web activity.

E. Monitor, analyse, and report on suspicious User activity, threats, and policy compliance for applications.

F. Configuration of policies in agreement with the Customer.

(iii) Secure Internet Access (SIA):

A. Interactive will deploy rules to route the Internet-bound traffic from remote Users through the SASE cloud for security inspection, including web filtering, threat protection, and data loss prevention (DLP).

B. Interactive will implement policy enforcements for different categories (e.g., blocking risky sites, enforcing compliance policies).

20.2 **Advanced Tier**

(a) If the CMS SOW states that the Customer has purchased the Cloud Delivered Security Services under the Advanced Tier, Interactive will provide all services described in the Standard Tier plus the following:

(i) Advanced Secure Web Gateway (SWG) and Inline Cloud Access Secure Broker (CASB):

A. DLP with custom classifier and, file-type controls.

B. Sanctioned/unsanctioned app controls via inline CASB.

C. Conditional policies.

D. Quarterly policy reviews with compliance mapping.

(ii) Advanced CASB API Protection:

A. Custom DLP.

B. Quarterly compliance reviews.

(iii) Secure Private Access:

A. Interactive will provide fast and secure remote access to specific services, applications, and data-based on clearly defined access-control policies. These applications may be deployed at a private data center or in the public cloud.

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

C. ZTNA for sanctioned private apps, identity-based access, posture checks.

D. Conditional access by risk, MFA enforcement, granular app segmentation, integration with IdP and EDR (customer-provided).

(iv) Data Loss Prevention (DLP):

A. Identify sensitive information across multiple on-premises and cloud-based systems.

B. Prevent the accidental sharing of data with vendor provided standard data templates.

C. Monitor and protect private data with vendor provided standard data templates.

20.3 **Service Exclusions:**

(a) The following exclusions apply to both the Standard and Advance Tiers of the Cloud Delivered Security Services:

(i) Traditional firewalls, VPN hardware, and network equipment outside of the SASE ecosystem.

(ii) Management of the physical servers, switches, and other on-premises hardware.

(iii) Full management of the Device itself, such as operating system updates, patching, and hardware repair.

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

(v) Advanced troubleshooting of infrastructure issues, or advanced issues the Customer may encounter.

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

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

(viii) Any regulatory compliance obligations, audits or data sovereignty guarantees.

(ix) Any liability for security breaches.

(x) SIEM Integration: Interactive can provide the Customer with Log management & collection for integration with Security Information and Event Management (SIEM) systems for centralized security insights. The Customer needs to purchase SIEM Service separately and is sold as part of Interactive’s Cyber portfolio.

(xi) Endpoint Detection & Response (EDR): Interactive can provide integration with EDR. The Customer needs to purchase the EDR Service separately and is sold as part of Interactive’s Cyber portfolio.

21 Project Transition (Onboarding Stage)

21.1 Interactive will perform the below set of activities during the Project Transition:

Phase	Services	Key Tasks	Detailed Activities
Phase 1	Planning and Preparation	Kick-off	Conduct a formal project kick-off meeting with stakeholders from Interactive and Customer. Discuss Business Goals for SASE and specific use cases.
		Requirement Gathering	○ Gather detailed requirements including compliance needs, critical applications, User groups, and performance expectations. ○ Collect current network documents, including asset lists and high-level network design (HLD). ○ Perform workshops to gather additional information as needed.
Phase 2	Discovery and Assessment	Current Environment Assessment	○ Perform a thorough audit of the Customer’s existing IT environment including network infrastructure, identity systems, security controls/policies. ○ Document network topology and traffic flows, identify User groups/roles, note any gaps.
		Network Design and Risk Assessment	○ Validate the HLD to ensure it accurately reflects the current environment. ○ Identify and document risks, such as outdated firmware or unsupported devices. ○ Create a report summarizing findings, asset validation, support contracts, and risks. ○ Define scope, policies and SLAs. ○ Verify all pre-requisites required for SASE integration.
Phase 3	Design & Initiation	Workshop Design Requirements	○ Solution workshops, architecture design, and planning documentation for SASE integration into Customer environment. ○ Interactive to work with Vendor to ensure best-practice SASE design. ○ Prepare a solution design document.
Phase 4	Build & Configuration	○ SASE Platform Configuration (Security Policies) ○ Network Integration (Connectivity Setup) ○ Integration with Monitoring Systems ○ User communication and Training Preparation	○ Setup and configure policies for the managed SSE components. ○ Setup Identity Integration with Customer’s IdP. This includes any Identity integration required for SASE authentication. ○ One time setup for identity and access management for Users and Devices.
Phase 5	Pilot Rollout and Testing	Phased Rollout, split into User groups	○ Deployment of the SASE agent to a pilot User group and execution of functional test cases (up to 10 use-case scenarios) to validate the solution.
		Hypercare	○ Interactive will provide on-site/remote cutover assistance for the pilot Users and address any issues.
Phase 6	Transition to Operations	Documentation and Handover	○ Create the final overall network design document. ○ Confirm and validate all network documentation prepared during the Onboarding.
		Service Transition	○ Transition service management to operations. ○ Complete transition to Business As Usual (BAU) operations.

21.2 Interactive requires the Customer to provide the following key documents:

- Asset list (device inventory, support status)

- Credential list (access methods and credentials)
- High-Level Design (network architecture and interconnectivity)
- As-built documentation (detailed device configurations, if available)

Note: Any major transformation or remediation will be scoped separately, and additional effort may be required if documentation is incomplete or inaccurate. The onboarding process ensures that all devices are managed, monitored, and secured according to SASE best practices, with a clear transition to operational support.

22 Service Level Agreement

22.1 This Service Level Agreement sets out the procedure for the Customer to follow when reporting an Incident and the applicable Service Levels that will be provided.

22.2 Incident Reporting Procedure

(a) If the Customer experiences an Incident, the Customer must take reasonable steps to ensure that the Incident is not within the Customer's Responsibility Domain before reporting the Incident to Interactive.

(b) If, after taking those steps, the Customer is satisfied that an Incident is within the Customer's Responsibility Domain, the Customer may report the Incident to the Interactive Service Desk in accordance with the procedure set out in clause 5

(c) When logging a Service Call, the Customer must provide the following information:

(i) Customer Name and Service ID affected by the Incident.

(ii) Description of the Incident.

(iii) Name and contact details of the person reporting the Incident.

(iv) Name and address of the Customer Location.

(v) Business / trading hours of the Customer Location.

(d) Interactive will issue all Incidents logged with the Service Desk with an Incident number. This Incident number will be the sole reference number for the Incident and will be referenced in subsequent communication from Interactive regarding the Incident.

(e) The Customer may log non-critical issues that do not affect the Service, but do require attention, by phone call or emailing the Service Desk. Interactive will provide an Incident number for all issues, including non-critical issues. Interactive will respond by email to all Incidents the Customer logs by email.

(f) Interactive, may acting reasonably charge the Customer a reasonable amount, based on the Standard Charge Out Rate, to diagnose an Incident if the Customer knew, ought to have known, or would have known following reasonable investigation, that the Incident was not caused by Interactive, or was caused by something within the Customer's Responsibility Domain.

22.3 Incident Classification

(a) Interactive will determine the severity of any reported Incident based upon the Customer's impact assessment, having regard to the urgency and impact factors in Table A and Table B. Interactive will then allocate a severity level in accordance with Table C.

(b) The Customer's callers to the Service Desk must define the level or urgency of the Incident in accordance with Table A and define the impact of the Incident in accordance with Table B.

(c) Notwithstanding the urgency or impact factors:

(i) Interactive will classify any Service Calls placed by the Customer by email or online as Severity 3 or 4 incidents; and

(ii) Severity 1 or 2 incidents Service Calls must be placed by the Customer by phone calls.

Table A – Urgency Factors

Critical	**High**	**Medium**	**Low**
Critical business function impacted.	Important business function is impacted.	Administration activities impacted.	Business function continues.

Table B – Impact Factors

Critical	**High**	**Medium**	**Low**
All Customer Users are affected.	All business unit or department Users are affected.	All team Users are affected.	Only an individual is affected.

Table C – Severity Level

Severity		**Impact**			
		Critical	High	Medium	Low
Urgency	Critical	SEV 1	SEV 2	SEV 2	SEV 3
	High	SEV 1	SEV 2	SEV 3	SEV 4
	Medium	n/a	SEV 3	SEV 4	SEV 4
	Low	n/a	SEV 4	SEV 4	SEV 4

22.4 Initial Impact Assessment

(a) Where there is doubt regarding impact to a significant number of Users or a few Users, Interactive will be conservative and classify the Incident initially at the next highest level. Interactive may adjust the Incident severity level later with a valid reassessment.

(b) Where the assessed severity does not reflect the Customer's requirements, the Customer may escalate the matter to Interactive's Contract Representative. This is the initial step before Interactive will assign a higher severity level.

22.5 Service Level – Response Time

(a) Interactive will use reasonable endeavours to respond to the Customer's Service Calls for the reporting of an Incident within the Response Time set out in Table D.

Table D – Response Time

Severity Level	**Response Time**
Severity 1 – Critical	< 30 minutes
Severity 2 – High	< 1 hour
Severity 3 – Medium	< 8 hours (Business Hours)
Severity 4 – Low	< 24 hours (Business Hours)

22.6 Service Levels – Restoration Time

(a) Interactive will use reasonable endeavours to Restore an Incident within the Restoration Time set out in Table E, to the extent the Incident is within Interactive’s Responsibility Domain.

(b) A Service may be Restored via temporary measures. Permanent corrective actions are not required for the Service to be deemed Restored.

(c) Incident Restoration

(i) The Restoration Time Service Level is conditional on Interactive or its representative having access to the Customer’s Device/ system and the Customer responsibilities being carried out.

(ii) Interactive will contact the Customer and confirm that the Service is operating satisfactorily after Restoring the Service.

Table E – Restoration Time

Severity Level	**Restoration Time**	
	Incident within Interactive’s Responsibility Domain, where Interactive is the Provider	Incident with a third party
Severity 1 – Critical	4 hours	N/A
Severity 2 – High	8 hours	N/A
Severity 3 – Medium	2 days (Business Hours)	N/A
Severity 4 – Low	4 days (Business Hours)	N/A

22.7 Excused Disruptions

(a) Notwithstanding any other provision of the Service Level Agreement, Interactive is deemed to have not breached a Service Level where Interactive's failure to achieve the relevant Service Level is directly or indirectly caused or contributed by:

(i) Third Party Fault;

(ii) Customer Events;

(iii) Planned Outage Periods;

(iv) Emergency Events;

(v) the Customer failed to provide access to their premises, Device, system or the Customer Location to repair an Incident, or failed to co-operate with Interactive as reasonably required to rectify the Incident;

(vi) the Customer has modified or changed any aspect of the original installation or configuration without Interactive's consent or used the Service improperly;

(vii) the Customer failed to notify Interactive of an Incident;

(viii) the Customer and the Customer's third parties failed to carry out their responsibilities; or

(ix) the information provided by the Customer was incorrect or inadequate, or if technical requirements are proven to be beyond the capabilities of the SASE Management Services.

23 Transition Out

23.1 If the Services are terminated for any reason, the parties shall consult and agree on the terms and responsibilities involved in transitioning out of the Services to the Customer, or a third party appointed by the Customer. If the Services are validly terminated by the Customer in accordance with the Agreement, Interactive will promptly comply with all reasonable requests and directions of the Customer in order to facilitate the transitioning out of the Services and Customer data so as to cause minimal interruption to ongoing services.

23.2 The Customer shall pay Interactive on a time and materials basis (with labour charged at the Standard Charge Out Rate), all reasonable costs and charges incurred by Interactive in relation to the transitioning out of the Services.

24 General

24.1 Interactive will provide the Services to the Customer either directly, via a third party engaged by Interactive on behalf of the Customer, or both.

24.2 Interactive may (acting reasonably) vary these Terms or Service Descriptions (as applicable) at any time provided that Interactive notifies the Customer of any proposed material variation in writing no less than 30 days in advance of any such variation and posts an updated version at www.interactive.com.au/terms-and-conditions or such other URL as may be used by Interactive and stated in the notice. The variation to the Terms or relevant Service Description will apply from the version date stated on that document, and by continuing to use the Services after that date, the Customer agrees to the varied Terms or Service Description.

24.3 If a variation is proposed in accordance with clause 24.2 that materially and adversely impacts the rights or obligations of the Customer under the Terms or relevant Service Description (including through the imposition of, or increase to, any fee or charge payable by the Customer beyond anything detailed in a Statement of Work, Master Services Agreement, these Terms, or a Service Description but excluding changes required by law or regulatory bodies or third party providers), the Customer may elect to remain on the then current version of the relevant Terms or Service Description (if possible) by giving fourteen (14) days written notice to Interactive. This notice must be given by the Customer to Interactive within thirty (30) days of Interactive notifying the Customer of the proposed variation. Where this election is made by the Customer the parties will sign an executable copy of the last agreed Terms or Service Description.

25 Definitions

25.1 The following definitions apply to the Agreement:

Acceptance Testing or Acceptance Test means the Customer’s testing of the software or hardware to confirm the systems is operational as per usual before and after Interactive management tools installation.

Active Directory means a database and set of services that connect Users with the Resources they need to get their work done.

Agreement means these Terms, the CMS SOW, the Master Services Agreement, and each applicable Service Description.

Change Management Process means the process described in clause 8.

CMS SOW means the statement of work for cloud and managed services entered into between Interactive and the Customer named in that statement of work.

Customer means Interactive’s customer named in the Statement of Work or other agreement for the Services.

Customer Events means any one or more of the following:

(a) any act or omission by the Customer;

(b) the Customer’s negligent, fraudulent or intentional acts or omissions;

(c) the Customer’s breach of the Agreement for Services; or

(d) the Customer’s equipment failing or any Incidents within the Customer’s Responsibility Domain.

Customer Location means the location of the Customer’s sites where Devices are located, as set out in the CMS SOW.

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

Due Diligence Stage comprises the Customer providing Interactive with access to its systems and supporting documentation; Interactive validating the Customer’s in scope systems and services; and the parties attending joint workshops.

EDR or Endpoint Detection and Response is a cybersecurity solution (also provided by Interactive as an optional service) that continuously monitors network endpoints like laptops, desktops, and servers for malicious activity, detects threats in real-time, and automates responses to contain and mitigate them.

Emergency Events means any one or more of the following:

(a) a Force Majeure event;

(b) unscheduled maintenance in cases of emergency or urgent Service interruption; or

(c) power interruptions.

Environment refers to a tenancy in Azure or a tenancy in AWS. For the avoidance of doubt each of these are separate environments and charged separately.

Further Term has the meaning given to it in clause 2.2(b).

Identity Provider (IdP) is a trusted system that manages and authenticates user identities, allowing them to securely access various cloud applications and resources. E.g. Okta, Microsoft Azure Active Directory, Google Workspace etc.

Incident means an issue affecting a Service that requires immediate attention, which may include degradation of the Service as further described in the Service Level Agreement.

Individual Term means, for the SASE Management Service, the individual term set out in the CMS SOW, commencing on the Service Start Date, as extended in accordance with these Terms.

ITIL Management means Information Technology Infrastructure Library, is a well-known set of IT best practices designed to assist businesses in aligning IT services with customers.

ITSM means Information Technology Service Management. It is how IT teams manage the end to end delivery of IT services to customers.

Maintenance Plan means a collection of tasks that perform maintenance on database objects to maintain those objects in a good state.

Major Incident means any unplanned event or condition—such as a critical system outage, significant cybersecurity breach, or data center failure—that materially disrupts the availability, integrity, or confidentiality of services and has a severe impact on business operations, regulatory obligations, revenue, or reputation.

Managed Services means the management services provided by Interactive as described in the relevant Service Description.

Management Tier means the tier of SASE Management Service that applies for a Device, Services and may be simple, standard, advanced or complex, as specified in the CMS SOW.

Master Services Agreement means the Master Services Agreement referred to in the CMS SOW.

MDR or Managed Detection and Response is a cybersecurity service (also provided by Interactive as an optional service) that combines technology and human expertise to monitor an organization's environment 24/7, detect threats, and respond to them in real time.

MFA means Multi-Factor Authentication. It is a core component of a strong identity and access management policy, in addition to a User name and password.

Microsoft Entra means identity and access solution for Azure Active Directory to provide secure access for the Customer.

Network Devices network device is an individual component of the network that participates at one or more of the protocol layers. This includes, but is not limited to, end devices, routers, switches, firewalls.

Network Management means simple, standard, advanced or complex management of the Network Devices, and includes any associated Services set out in the CMS SOW.

Onboarding Stage consists of implementing the Solution; tracking progress against the Project plans and Acceptance Testing.

Personnel means in the case of Interactive, its employees or contractors who perform the Services and in the case of the Customer its employees who receive the benefit of the Services.

Planned Outage Period means a period during which time the Services may not be available, or that performance of the Services may be impacted**.**

Platform means any hardware or software used to host an application or service.

Platform Fee means the monthly Service Fee payable per Environment by the Customer to avail the Platform Management Services from Interactive.

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

Project means all work to be performed during the Due Diligence Stage, the Onboarding Stage and Acceptance Testing to deliver the Solution to the Customer in accordance with these Service Terms and the CMS SOW.

Project Manager means the Interactive or Customer staff member responsible for delivery of the CMS SOW.

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

Rate Card means the Cloud Rate Card found at https://www.interactive.com.au/terms-and-conditions/ or such other URL as may be used by Interactive from time to time.

Resource means hardware, software, virtual appliances, any underlying infrastructure which is managed by Interactive Anywhere Service.

Response Time means the time from when Interactive receives a Service Call from the Customer to when a technical Interactive Personnel begins investigating the Incident to conduct initial diagnosis. Where possible, Interactive will provide a status advice to the Customer with an indication of the nature of the Incident and estimated time to restore the Service.

Responsibility Domain means, in relation to a party, equipment or networks owned or managed by the party, or anything provided by a third party engaged by the party.

Restoration or Restore means, in respect of an Incident, the return to normal Service operation, which may be achieved bytemporary measures.

Restoration Time means the time taken from when Interactive receives a Service Call from the Customer, until the time the Service is Restored.

RMA means Return Material Authorisation and is required to return equipment to vendor.

Services means the services provided by Interactive to the Customer under a Statement of Work.

Service Call means contact made by or on behalf of a Customer to the Interactive Service Desk which may relate to an Incident or a Service Request.

Service Catalogue means the catalogue of services and associated prices for repeatable Services that can be provided by Interactive, as may be updated from time to time

Service Description means the description of, and terms applicable to, certain Services.

Service Desk means the single point of contact between customers and Interactive to handle communication with the Customer.

Service Levels means the service levels specified in the Service Level Agreement.

Service Level Targets means the targets that apply to the Managed SASE Services. Service Request is defined in clause 6 of these Service Terms.

Service Request means a request for service from the Customer, which may be a Simple Service Request or Complex Service Request, that is a move, add, change or delete to the Managed SASE Services.

Simple Service Request Entitlement means the number of Simple Service Requests that the Customer is entitled to raise within a month included in the Service Fee as set out in the CMS SOW.

Service Start Date means, for the Services, the earlier of the date notified by Interactive in accordance with clause 7.2 or 7.11 for all Services, or the date the Customer accepts the results of Acceptance Testing for all Services.

Solution means the proof of concept or technical design of the Services contained in the CMS SOW.

SSO means Single Sign On. It is an authentication method that enables Users to securely authenticate with multiple software systems using a single set of credentials.

Third Party Fault means any one or more of the following:

(a) any act or omission by any third party;

(b) failure by the provider of services utilised by the third party to deliver Services; or

(c) any event or component of the Service beyond Interactive's control, which may include breakdowns of machinery or equipment, facilities outside of Interactive's control or telecommunications failure.

(d) the Incident is wholly or partly dependent on a third party for Restoration;

Tier of Service means the level of Managed SASE Services, which may be Platform only, or Platform and either Standard or Advanced as detailed in the CMS SOW.

Tools means the tools to be used to manage the in-scope services.

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

25.2 Unless the context otherwise requires, words and expressions defined in the Master Services Agreement have the same meaning in these Terms and any terms not defined herein have the meaning set out in the Master Services Agreement.