

SCHEDULE P: SERVICE DEFINITION FOR SECURE ACCESS SERVICE EDGE (“SASE”) SERVICE

1. SASE Service Description

The Vysiion SASE Service comprises of the following mandatory components, to the extent set out on the Order Form:

- Overlay Bandwidth;
- Firewall as a Service / Secure Web Gateway;
- Vysiion Implementation (Configuration and Migration);
- Vysiion Management; and
- Orchestration Portal.

One or more of the following optional components will also be provided as part of the SASE Service, to the extent set out on the Order Form:

- Provision of an SD-WAN Service (in the form of Hardware, Software and/or Licensing);
- VPN Connection;
- Provision of Software Defined Perimeter (SDP) Users (in the form of Licensed Software);
- Provision of Enhanced Security Service Edge (SSE) Licencing (in the form of Licensing);

Each as further described below.

All elements of the SASE Service are securely connected via the SASE Cloud Platform, with all traffic having the appropriate configuration applied as set in the Orchestration Portal.

1.1 Overlay Bandwidth

Overlay bandwidth is required for network connectivity to the SASE Service, and can be purchased in two ways:

- Site based: Each Customer Site will have a set amount of bandwidth available to be used from the Customer Site as specified on the Order Form.
- Solution Based: will have an aggregate amount of bandwidth for a specified geographical region to be used across all Customer Sites within that geographical region, as specified on the Order Form.

For the avoidance of doubt, this service component is subject to Charges (either per Site or at Solution level) as set out on the Order Form.

1.2 Firewall as a Service/Secure Web Gateway

Cloud-based firewalls will be provided as part of the SASE Service. These firewalls will be setting rules for traffic to flow or be blocked between: Site to Site, Site to Internet and Internet to Site traffic. It analyses traffic at layer 7 inbound and outbound of the SASE networks.

A basic level of configuration and security policy development in consultation with the Customer is included. Vysiion maintains full access to the firewall and carries out management using the SASE portal. Read Only Access will be provided to the Customer.

A managed firewall is part of an overall security policy and does not guarantee total security (for example, vulnerabilities may exist in traffic flows that are permitted by the firewall policy).

For the avoidance of doubt, this service component is not subject to its own Charges.

1.3 SASE Implementation

Vysiion shall work remotely to complete the configuration of the SASE Service, this comprises the following tasks:

- Scoping workshop to agree on low-level design.
- Pre-configure SD-WAN Edge Devices and set up the Orchestration Platform.
- Remotely migrate the SD-WAN Edge Devices into the Orchestration Platform as it becomes live.
- Set up reporting and monitoring of the SD-WAN Edge Devices into Vysiion systems.
- Solution testing including connectivity between site and orchestration platform and SD-WAN functionality.
- Set up SDP Users on the Orchestration Platform.

For the avoidance of doubt, this service element is subject to Charges as set out on the Order Form.

Certificate Installation

The SASE Service requires a digital certificate to be installed in the Trusted Root Certification Authority on all devices using the network. Unless provided by the Customer, the certificates are provided with this service during implementation.

It will be the Customer’s responsibility to ensure the certificates are installed and up to date on all relevant devices

accessing the network.

Out of Hours Migration

If requested, Vysiion shall work remotely to perform SASE Service implementation activities on a Working Day, but outside of Normal Business Hours (“Out of Hours Migration”) for additional charge. The number of Customer Sites that are included for Out of Hours Migration (if applicable) shall be as stated on the Order Form.

1.4 Management

Vysiion management comprises of:

- 24x7x365 remote support from the Vysiion Service Desk to the Customer’s Service Desk;
- Remote hardware monitoring of any in-scope SD-WAN Edge Devices;
- Change Management.

The Customer shall undertake reasonable on-site troubleshooting activities as requested by Vysiion. If a fault is identified as being with equipment or service which does not form part of this Service e.g third-party connectivity service, computer, printer or tablet then it will be the Customer’s responsibility to resolve the issue with the equipment or third-party service, unless the Customer has a valid support contract in place for that equipment with Vysiion. Charges for Management shall apply from the date that the first SD-WAN Edge Device or VPN Connection is handed over to the Customer or the Software licencing begins (whichever occurs first).

Change Management

A total of 10 hours of engineering time per calendar month to effect changes to the SASE Service shall be provided at no additional charge, with each change accounting for at least 1 hour of engineering time. For additional engineering hours, the Vysiion Service Desk will advise the cost and will need Customer acceptance via email that the cost has been accepted before proceeding with the change. Changes requested will normally only be carried out during Normal Business Hours.

Change request target lead times as follows:

- Standard and Normal changes – 48 hours
- Emergency – 24 hours*

**Emergency Changes should be reserved to restore service, prevent a service impact, or restore a degraded service as determined by Vysiion acting reasonably.*

For the avoidance of doubt, this Management service element is subject to Charges as set out on the Order Form.

1.5 Orchestration Portal

Vysiion uses a SASE Orchestration Portal provided via the vendor, to allow for a central control and management plane for the management of networking across the SASE Service, the changing or adding of sites or users, modification of security policies and reporting. The portal can be a dedicated appliance, located at a Customer Site, or in Vysiion Data Centres, or can take the form of a SaaS-based platform hosted by the Vendor. By default, Vysiion fully manages configuration, and provides ‘read only’ access to the features and reporting metrics in-built within the Portal. The Customer will be provided with multi-factor authentication-based read-only access to the SASE Orchestration Portal for the number of users specified on the Order Form (if any).

For the avoidance of doubt, this service component is not subject to its own Charges.

1.6 SD-WAN Service

The SD-WAN Service provides an overlay service, configured on SD-WAN Edge devices and clients which terminate the data plane for customers’ network services delivered from central and remote sites to the SASE Cloud Platform. See Schedule O for full details of the SD WAN Service.

For the avoidance of doubt, this service element is subject to per Site Charges as set out on the Order Form.

1.7 VPN Connection

The Customer can use a VPN connection over the internet instead of a SD-WAN Edge device to connect to the SASE Service from a firewall or VPN device. Vysiion will provide configuration settings for the firewall or VPN device as part of the SASE Service.

It will be the responsibility of the Customer to configure all Customer-owned devices for connection into the SASE Service; settings for the VPN connection will be provided by Vysiion at time of SASE Service deployment. However, where the Customer-owned firewall or VPN device is managed by Vysiion under some other Vysiion service, this VPN connection will be configured by Vysiion.

For the avoidance of doubt, this service element is subject to per Site Charges as set out on the Order Form.

1.8 Software Defined Perimeter (SDP) Users

SDP user licences are for users accessing the SASE overlay network via their endpoint device directly such as a phone, tablet, laptop or server for example. These devices do not need to be located on the Network behind a SASE device.

SDP user licences are purchased on a per user basis and will connect via a software client on an endpoint device to connect into the SASE Service. The number of users/licences will be specified on the Order Form.

It will be the responsibility of the Customer to deploy all SDP agents to the relevant devices.

For the avoidance of doubt, this service element is subject to Charges as set out on the Order Form.

1.9 Enhanced SSE Licencing

These following individual enhanced SSE aspects are available to be licensed and are only included if the relevant option is taken as shown on the Order form.

Next Gen Malware Protection

For active inspection of files being sent over the WAN and Internet traffic for Malware and other malicious files.

Licensing will be for a set amount of bandwidth specified on the Order Form.

Intrusion Prevention System (IPS)

For the inspection of the WAN and internet traffic, to identify a compromised system or malicious traffic traversing the Customer's network.

Licensing will be for a set amount of bandwidth specified on the Order Form.

Cloud Access Security Broker (CASB)

For providing insights and control over cloud SaaS based application usage within the Customer's organisation.

Data Loss Protection (DLP)

For protecting sensitive information from being uploaded to or extracted from the cloud or physical data centres. This service inspects traffic to identify file types and will take a defined action when found.

RBI

RBI (Remote Browser Isolation) is for protecting users from accessing newly registered or unclassified websites. A website is simulated and streamed from the SASE service to the user rather than running the website on the end-device's browser itself.

For the avoidance of doubt, each type of SSE license taken is subject to Charges as set out on the Order Form.

2. Service Demarcation Point (SDP)

The Demarcation Point is the point up to which Vysiion's SASE Service obligations apply and is the point up to which the SASE Service Level Agreement covers.

When a SD WAN Service is in scope, the Demarcation Point at each Site is on the LAN facing port of the SD-WAN edge device.

When a VPN Connection is in scope and Vysiion is managing the relevant firewall or VPN device, the Demarcation Point at each Site is the LAN-facing port of the managed firewall or VPN device.

When a VPN Connection is in scope but Vysiion is not managing the relevant firewall or VPN device, the Demarcation Point at each Site is the SASE Cloud Platform.

In all other cases, the Demarcation Point is the SASE Cloud Platform.

Vysiion are dependent on the Cato platform for this service, the Cato platform status can be viewed at <https://status.catonetworks.com/>. Vysiion are not responsible for outages on the Cato platform.

3. Target Service Commencement Date

SASE Service 30 Working Days¹²³

¹From order acceptance

²The Target Service Commencement Date is subject to equipment vendor lead times where physical SD-WAN Edge Devices are in scope.

³This lead time does not include the underlying connectivity.

4. SASE Service Level Agreement

Availability is defined, for each Customer Site, as the time which a Customer Site is active, enabled and has reasonable access to the SASE Service (as determined by Cato). Customer Site for the purpose of this Service Level Agreement means a location connected to the SASE Service via either an SD WAN Service or a VPN Connection. For the avoidance of doubt, but without limitation and in addition to the Excused Reasons set out in Section 5.2 of the Main Body of this Service Document, this excludes time that the Customer Site is unable to access the SASE Service due to any of the following: (a) planned and/or emergency works; (b) any failure of underlying connectivity services; (c) any failure of SD

WAN Edge Devices and/or managed firewall / VPN devices (d) Any systemic Internet failures; (e) Any failure in the Site hardware, software or network connection; (f) Site’s bandwidth restrictions; and/or (g) anything outside of the direct control of Vysiion and/or the underlying provider, Cato Networks.

Target Availability

	Target Availability
SASE Service	99.999%

Service Credits

	Measure	Service Credit*
Availability	>0.1 Below Target	5%
	>2 Below Target	7%

** The Service Credit is applied as a percentage of the aggregate Monthly Charge for the elements of the SASE Service being charged for at the affected Customer Site only (for the avoidance of doubt this excludes any elements that are charged for on a non per-Site basis).*

5. Additional Terms

The following terms apply to the provision of the SASE Service by Vysiion in addition to Vysiion’s General Terms and the terms and conditions set out in the main body of this Service Document.

- 5.1 In relation to the SASE Service, the Initial Term is actually a fixed period calculated from Service Commencement Date. Upon expiry of this period, the SASE Service will automatically cease to be provided, without notice, unless the Customer re-contracts with Vysiion for the continued provision of the SASE Service.
- 5.2 The planned works notice provision in Section 3.3 of the main body of this Service Document does not apply to the SASE Service (including for the avoidance of doubt any SD WAN Service forming part of it). Vysiion shall provide the Customer with as much notice as is reasonably possible of planned works on the SASE Service (including any SD WAN Service) following notice of the same from Cato Networks (it being noted that Vysiion could get as little as 48 hours’ advance notice from Cato Networks).
- 5.3 The Customer acknowledges and accepts that the underlying provider, Cato Networks, hosts the Service and may update the functionality, user interface, usability and other user documentation, training and educational information of, relating to the SASE Service, from time to time, in its sole discretion. The Customer agrees that Cato Networks may make necessary technical or other changes to the SASE Service and the provision of the SASE Service on an as-needed basis. Where any such change would adversely and materially affect Customer, the Customer will be notified in advance.
- 5.4 The Customer shall contact Vysiion promptly if (i) account information is lost, stolen, or disclosed to an unauthorized person; (ii) the Customer reasonably believes that the account has been compromised, including any unauthorized access, use, or disclosure of account information; or (iii) any other breach of security in relation to its passwords, usernames, access information, or the SASE Service that may have occurred or is reasonably likely to occur.
- 5.5 The Customer shall not (i) ship, transfer, or export the SASE Service or any component thereof or use the SASE Service in any manner prohibited by law, including without limitation to, sell, distribute or, export the SASE Service (or any element thereof) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Lebanon or Syria, or otherwise in violation of any export or import restrictions, laws or regulations of the U.S. or Israel or any foreign agency or authority. The Customer agrees to the foregoing and warrants that it is not located in, under the control of, or a national or resident of any prohibited country or on any prohibited party list; (ii) contest Cato’s Intellectual Property Rights in the SASE Service and any other Cato materials; (iii) remove or add any labels, notices or logos to the SASE Service, (iv) perform any act or be responsible to any omission that is illegal, including, without limitation, those enforcing censorship, privacy, government authority restrictions, or by accessing any blocked services, or in Cato’s discretion otherwise jeopardizes, destabilizes, interrupts or encumbers the SASE Service and/or Cato’s Network or their servers and/or has a detrimental impact on Cato and/or Cato’s Intellectual Property Rights and/or Cato’s Network.
- 5.6 Whether Customer has violated any of the limitations set forth in Clause 5.5 above shall reside within Cato’s sole discretion. If Cato determines a violation has occurred, the Customer will be notified of the violation and Customer shall be required to cease the violation immediately. Cato may also determine in its sole discretion whether to suspend or block the Customer account as a result of such violation. Cato shall use such remedy if and when such violation represents an imminent threat to Cato’s Network or if so directed by a court of

competent authority. In such cases: (i) Cato will suspend the account only to the extent reasonably necessary to prevent any harm to Cato's Network; (ii) reasonable efforts will be used to promptly contact Customer and give Customer the opportunity to promptly resolve the issues causing the suspension of the account; and (iii) Cato will reinstate any suspended part of the account immediately after any issue as above-mentioned has been resolved, provided if Cato determines that any such violation was wilful or is unable to be adequately remedied, the SASE Service may be immediately terminated.

- 5.7 The Customer shall use the SASE Service in accordance with any Cato documentation made available and/or provided to Customer, and as may be updated from time to time, and in compliance with the applicable operating instructions and all applicable laws and regulations and for no purpose other than as specifically authorized in the Cato documentation, including without limitation, the Customer shall not use the SASE Service for the purpose of circumvention of government censorship, laws or regulations.
- 5.8 The Customer will enable and permit Cato (and/or its third party contractors) to process Customer data, which includes network traffic including traffic data and URL(s), IP address(es) used in connection therewith to support the Services, all in accordance with Cato's Data Processing and Privacy Agreement available at: <https://www.catonetworks.com/cato-networks-data-processing-and-privacy-agreement/>; (the "Cato's Data Processing Agreement") and Cato's Privacy Policy (<https://www.catonetworks.com/privacypolicy/>) (the "Privacy Policy").
- 5.9 The Customer will comply with all applicable privacy laws and regulations (including all registration and notice requirements), inclusive of the Cato Data Processing Agreement and the Privacy Policy; and the Customer will obtain all applicable consents required by law for data processing by Cato of personal information submitted by Customer, if any.
- 5.10 THE SASE SERVICE IS NOT DESIGNED FOR USE WITH CRITICAL OR LIFE SAVING INFRASTRUCTURES, SYSTEMS THAT CONTAIN OR PROTECT AGAINST DANGEROUS OR HAZARDOUS MATERIALS OR FORCES, NATIONAL SECURITY PURPOSES OR NUCLEAR, CHEMICAL, OR BIOLOGICAL WEAPONS AND THE CUSTOMER SHALL NOT USE IT FOR SUCH PURPOSES.