SCHEDULE O: SERVICE DEFINITION FOR FORTISASE™ SERVICE

1. FortiSASE™ Service Description

The Vysiion FortiSASE™ Service is a cloud-based Security Service Edge (SSE) delivered to the Customer through a network of geographically distributed Fortinet Points of Presence (PoPs) within the FortiSASE™ infrastructure. Customer traffic is processed, inspected and routed within the FortiSASE™ infrastructure.

1.1 The FortiSASE™ Service comprises of the following mandatory components:

- Vysiion Implementation (Configuration and Migration);
- Vysiion Management; and
- Provision of the FortiSASE Licencing.

All elements of the FortiSASE™ Service are connected via the Orchestration Portal.
The components detailed above will be specified on the Order Form.

1.1A Implementation

Vysiion shall provide the implementation services for the FortiSASE™ Service remotely, unless stated otherwise on the Order Form.

The provisions set out in this section shall apply as the standard position for all FortiSASE™ implementations unless the Customer is notified otherwise in writing by Vysiion.

Implementation shall comprise:

- A scoping workshop to confirm the implementation requirements, responsibilities, migration approach and low-level design.
- Provisioning and configuration of the Customer's FortiSASE™ tenant and purchased SSE licences.
- Configuration of the operating region and data residency preferences selected by the Customer, subject to availability within the FortiSASE™ platform.
- Integration with the Customer's identity provider, subject to compatibility with FortiSASE™, as confirmed by Vysiion.
- Configuration and deployment of the agreed network access and security policies.
- Configuration of the FortiSASE™ security capabilities included within the purchased Service.
- If applicable, configuration and deployment of the FortiClient application to the agreed Customer endpoints and enrolment of those endpoints with FortiSASE™.
- If applicable, configuration of Zero Trust Network Access, including agreed zero trust tags, application access policies and device posture checks.
- If applicable, reconfiguration of the Edge Devices required to connect Customer Sites to FortiSASE™.
- Where SD-WAN Edge devices are included within the agreed scope, remote integration of the applicable Edge Devices into FortiSASE™ at the point of operational readiness.
- Configuration of agreed connections to Customer Sites, data centres, cloud environments and private applications.
- Configuration of monitoring and reporting within Vysiion's monitoring systems.
- Testing that agreed users can successfully authenticate with FortiSASE™ and access an agreed internet resource.
- Where applicable, testing access to agreed private applications and validation of the agreed security policies.
- Handover of the implemented FortiSASE™ Service into Vysiion's support services team.

1.1A.1 Customer Responsibilities

The Customer shall:

- Assist with all reasonable request to provide the information requested by Vysiion including but not limited to complete and accurate details of its users, user groups, devices, applications, domains, security policies, incident resolution and access requirements.
- Confirm the users, user groups and devices to which the SSE licences and security policies shall apply.
- Provide access to, and appropriate administrative support for, any Customer managed identity, authentication, cloud, application or endpoint management platforms required for the implementation.
- Ensure that any Customer or third-party identity provider, directory service, application or authentication service required for the SSE Service is available and appropriately configured.
- Provide the information and access required to establish connections to Customer Sites, data centres, cloud environments and private applications.
- Ensure that any circuits, connectivity or third-party services not supplied or managed by Vysiion are installed, operational and available for testing.
- Deploy any required endpoint software or configuration to Customer devices unless expressly included within the Services supplied by Vysiion.
- Ensure that Customer devices meet the applicable technical and software requirements.
- Provide appropriate technical contacts and access to the Customer's systems where required.
- Approve the low-level design, security policies, implementation plan and change windows within the agreed timescales.
- Provide reasonable assistance during migration, testing and validation.
- Not unreasonably refuse a change to Service Credit entitlement where non-standard configurations are applied at the Customer's request.
- Implement and maintain all necessary subscriptions, permissions, clearances, rights, proper controls and processes to allow the Customer to receive the Services.

Any delay or additional work resulting from the Customer's failure to meet these responsibilities may affect the implementation dates and may be subject to additional Charges.

1.1A.2 Exclusions

Unless Vysiion advises the Customer otherwise, the SSE implementation excludes:

- Configuration, deployment or migration of SD WAN Edge Devices.
- Configuration or deployment of LAN switches, wireless access points and associated Management Platforms.
- Structured cabling, power installation or changes to the Customer Site's physical infrastructure.
- Delivery, installation or remediation of connectivity or third-party services.
- Deployment of endpoint software to Customer devices.
- Configuration or remediation of Customer managed identity providers, directory services or endpoint management platforms.
- End user device configuration, remediation or support.
- Application remediation, configuration or optimisation.
- Discovery or classification of Customer applications, users or data.
- Creation or review of security policies beyond those agreed for the SSE Service.
- Migration of configurations or policies from existing third-party security platforms.
- Additional site visits or professional services outside the agreed implementation scope.

Where other services form part of the wider solution, the applicable implementation activities, responsibilities and exclusions shall be as set out in the Order Form and relevant Service Schedule.

Any activities requested outside the agreed scope shall be subject to change control and may incur additional charges or affect the agreed delivery timescales.

1.1A.3 Testing and Completion

Vysiion shall test the implemented SSE Service against the following:

- Implementation shall be considered complete when:
- The purchased SSE licences have been provisioned and configured.
- The agreed identity and authentication integrations have been configured.
- The agreed access and security policies have been configured.
- The agreed connections to Customer Sites, data centres, cloud environments and private applications have been configured.
- The agreed migration and cutover activities have been completed.
- The applicable implementation activities and tests have been completed.
- The SSE Service has been handed over to Vysiion's support services team.

Vysiion shall confirm completion of the applicable implementation activities and tests.

Following handover, fault management and troubleshooting shall be undertaken in accordance with the Management provisions of this Service Document.

1.1B Management

Vysiion management comprises of:

- 24x7x365 remote support from the Vysiion Service Desk; and.
- 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 the FortiSASE™ 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 (or service as applicable) with Vysiion. Charges for management shall apply from the date that service is handed over to the Customer or the Software licencing begins (whichever occurs first).

1.1B.1 Change Management

A total of ten (10) hours of engineering time per calendar month to effect changes to the FortiSASE™ Service shall be provided at no additional charge, with each change accounting for at least one (1) hour of engineering time. For additional engineering hours or priority changes that sit outside change request target lead times, 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 are 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.

1.1B2 Orchestration Portal

Vysiion leverages a vendor-provided FortiSASE™ orchestration portal as the central platform for managing remote user access, security, and reporting across the FortiSASE™ Service. This portal takes the form of a SaaS based platform hosted by the vendor. Vysiion fully manages configuration and provides 'read only' access to the features and reporting metrics in-built within the Portal.

1.1B.3 SD-WAN Service

If included within the scope of Services provided to Customer, the SD-WAN Service provides an overlay network configured on SD-WAN Edge devices. Full details of the SD-WAN Service are set out in Schedule M.

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

1.1C. FortiSASE™ licensing

Vysiion offers three variants of FortiSASE™ User licenses:

- FortiSASE™ Standard Tier;
- FortiSASE™ Advanced Tier; and
- FortiSASE™ Comprehensive Tier.

The FortiSASE™ Standard Tier and FortiSASE™ Advanced Tier licences each require a minimum of fifty (50) users.

Each User licence type:

- is subject to monitoring and throttling of User bandwidth access ; and
- will include connectivity for up to four (4) FortiSASE™ PoPs located only in Fortinet cloud.

The number of users/licences will be specified on the Order Form.

FortiSASE™ Standard Tier: SIA, SSA, and ZTNA functions are included in the User Subscription License.

FortiSASE™ Advanced Tier: The Advanced license includes digital experience monitoring and access to additional FortiSASE™ PoP locations in addition to the features included in the Standard license.

FortiSASE™ Comprehensive Tier: This license provides the same features included in the Advanced license and includes the following:

- Up to one (1) FortiSASE™ PoPs located in either Fortinet cloud or public cloud where the Customer procures up to ninety-nine (99) user licenses
- Up to two (2) FortiSASE™ FortiSASE™ PoPs located in either Fortinet cloud or public cloud where the Customer procures between one hundred (100) and one hundred and ninety-nine (199) user licenses
- Up to four (4) FortiSASE™ PoPs located in either Fortinet cloud or public cloud where the Customer procures at least two hundred (200) user licenses.

For the avoidance of doubt, the abovementioned PoPs in respect of the FortiSASE™ Comprehensive Tier are not in addition to the four (4) PoPs provided under lesser tiers.

- Additionally, the FortiSASE™ licence enables the option to purchase an add-on via the FortiSASE™ Global Add-On (as described below) offering Global Security PoP coverage. Activation of this feature requires a separate FortiSASE™ Global PoP license, subject to scoping and must be specified on the Order Form.

1.1C.1 Secure Internet Access (SIA)

SIA is delivered as a component of the FortiSASE™ licensing. SIA provides security controls for access to internet resources, including but not limited to websites, web-based applications, and other internet-hosted content.

SIA leverages Next-Generation Firewall capabilities, including and not limited to

- SSL Inspection: For the decryption and inspection of encrypted WAN and internet traffic, to identify concealed threats, malicious payloads, or compromised communications traversing the Customer's network
- Inline Antivirus: For the real-time inspection of files and content across WAN and internet traffic, to detect, block, and prevent the delivery of malware to end users within the Customer's network.
- Intrusion Prevention: For the inspection of the WAN and internet traffic, to identify a compromised system or malicious traffic traversing the Customer's network.
- Web Filtering: For the inspection of web content to protect users from malicious sites and manage web usage.

- DNS Filtering: For the inspection and control of DNS traffic, to enforce access policies based on category, reputation, and security risk across the Customer's network.
- Botnet C&C Filtering: For the inspection of outbound traffic to identify and block communications between infected systems and botnet command-and-control servers within the Customer's network.

There are two methods of access for SIA:

- Agent-based: The FortiClient app is installed on supported end user device platforms.
- Agentless: Supported end user device platforms forward only HTTP or HTTPS traffic to the FortiSASE™ Secure Web Gateway, without the need for an agent-based software client.

1.1C.2 Secure SaaS Access (SSA)

- SSA is delivered as a component of the FortiSASE™ licencing. SSA provides security controls for access to Fortinet predefined SaaS applications, including but not limited to Microsoft 365, Dropbox, and Salesforce. SSA leverages Inline Cloud Access Security Broker (CASB) functionality to enforce granular security policies.
- Data Loss Prevention (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.
- Inline CASB: Application Control and Web Filtering functions combine as an Inline-CASB, inspecting SaaS traffic as it passes through the FortiSASE™ PoP.
- *Note that FortiCASB remains a separate product and is not included, only native Inline-CASB is provided with this Service. Unless mentioned in Order Form.*

1.1C.3 Add on Licences

The FortiSASE™ Service can be complemented by the following, chargeable, optional add-ons which shall be detailed on the Order Form where applicable:

1.1C.3.1 FortiGate SPA: FortiSASE™ Secure Private Access ("SPA") provides remote users with secure access to private enterprise applications. SPA is included as part of the SD-WAN Service bundle, and is supported on eligible FortiGate devices, subject to license availability, as specified on the Order Form.

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

1.1C.3.2The FortiSASE™ Global Add-On: Enables access to additional Fortinet FortiSASE™ points of presence (PoP).

2. Service Demarcation Point (SDP)

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

When an SPA connection is in scope and Vysiion is managing the firewall at the remote-end of the SPA connection, the Demarcation Point at each Site is the LAN-facing port of the managed firewall.

When an SPA connection is in scope, but Vysiion is not managing the firewall, the Demarcation Point at each Site is the FortiSASE™ PoP.

When a VPN connection is in scope and Vysiion is managing the 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 remote firewall or VPN device, the Demarcation Point at each Site is the FortiSASE™ PoP. In all other cases, the Demarcation Point is the FortiSASE™ PoP.

Vysiion is dependent on Fortinet's FortiSASE™ platform for this Service. The FortiSASE™ platform status can be viewed at https://status.FortiSASE™.com/. Vysiion cannot be held responsible for outages on the FortiSASE™ platform.

3. Target Service Commencement Date

FortiSASE™ Service 30 Working Days[1][2][3]

1. *From order acceptance*
2. *The Target Service Commencement Date is subject to equipment vendor lead times where physical edge devices are in scope.*
3. *This lead time does not include any additional time required for delivery of the underlying connectivity.*

4. FortiSASE™ Service Level Agreement

4.1 Availability is defined as the ability to accept the Customer's incoming packets, apply customer configured security controls (as delivered by the FortiSASE Service) and transmit processed packets to the internet.

Availability is calculated as the average percentage of the time during a calendar month the Service is available to the Customer excluding any time covered by Excused Reasons. It is subject to the Customer complying with the terms of this Service Document.

4.2 For the avoidance of doubt, and in addition to the Excused Reasons set out in Section 6.2 of the main body of this Service Document, Vysiion will not be liable for any time that the Customer's remote user is unable to access the FortiSASE™ Service due to any of the following reasons ("Excused Reasons"):

a) scheduled maintenance or emergency maintenance;
b) Customer exceeding the subscribed Service entitlement;
c) When a non-standard Customer requested configuration or Data Transfer Daily Enforcement Allocation is in place;
d) When the Service provided is free of charge, for evaluation or proof of concept purposes, or bundles as part of another service with the intention of being a seed or sample;
e) Customer's failure to adhere to Vysiion implementation, support processes and procedures;
f) acts or omissions of the Customer, its employees, agents, third party contractors or vendors or any third party accessing the Service;
g) any violations of the Customer responsibilities defined herein;
h) any event not wholly within the control of the underlying provider, Fortinet;
i) negligence or wilful misconduct of the Customer, or others authorized by the Customer to use the Services provided by Vysiion;
j) any failure of any component for which Vysiion is not responsible, including but not limited to all Customer´s infrastructure, electrical power sources, networking equipment, computer hardware, computer software or data;
k) any failures that cannot be corrected because the Customer, its systems or networks are not reasonably accessible to Vysiion. It is the Customer's responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details;
l) any failure of underlying connectivity services (including but not limited to systemic internet failures);
m) any failure of edge devices and/or managed firewall / VPN devices;
n) any failure in the Site hardware, software or network connection including but not limited to third party DNS services;
o) suspension or termination of Service by the underlying supplier (Fortinet) due to Customer's breach of any provision of the Fortinet EULA (defined below);
p) Site's bandwidth restrictions; and/or
q) anything outside of the direct control of Vysiion and/or the underlying provider, Fortinet.

4.3 Target Availability

	Target Availability
FortiSASE Service	99.999%

4.4 Service Credits

	Measure	Service Credit

Availability	>0.1 Below Target	10%
	>1 Below Target	15%
	>2 Below Target	20%

Service Credits shall not exceed 20% of the applicable Monthly Charge in any calendar month. In addition, the aggregate Service Credits awarded for the affected Service at the affected Customer Site shall not exceed the equivalent of 60 days' charges during any calendar year. Once this annual limit has been reached, no further Service Credits shall be payable for the remainder of that calendar year.

The Service Credit shall be applied only to the proportion of the Monthly Charge attributable to the individual user or users directly affected by the Availability failure. Where charges are not itemised per user, the applicable charge shall be calculated by dividing the Monthly Charge by the total number of licensed users. Under no circumstances shall a failure affecting an individual user result in a credit against the Monthly Charge for the entire Service or Customer Site.

4.5 Service Credits Claim Process

Notwithstanding section 6.3 of the main body of this Service Document, Service Credit claims must be submitted monthly in arrears to customerservices@vysiion.co.uk within five (5) days after the end of the month in which the failure to meet the target service level occurred. Apart from the reduced period specified, all other aspects of section 6.3 of the main body of this Service Document applies.

Any claim to Service Credits shall immediately cease with the expiry of the Service including when the Service is not renewed in accordance with the Contract.

5. Additional Terms

5.1 In the event that the continued provision of the Service to the Customer may compromise the security of the Service or Vysiion's systems, networks or reputation, the Customer agrees that Vysiion may temporarily or permanently suspend the Service to the Customer at Vysiion's sole discretion without liability. The Customer accepts and acknowledges that: (a) Vysiion shall not be liable for any damages, fines, claims, costs or expenses incurred or suffered by the Customer or any third parties as a result of or in connection with the breach of these warranties; and (b) it shall fully indemnify and hold Vysiion harmless from and against any and all claims, liabilities, losses, damages, penalties or fines, including all reasonable legal fees, arisen directly or indirectly as a consequence of the breach of these warranties.

5.2 Following termination or expiry of the Service subscription (or at the end of agreed Service evaluation period, if applicable), Vysiion will retain the configuration and any associated data for up to a period of fourteen (14) days to allow data collection or service re-initiation. Once such period is elapsed, the Customer's instance will be deleted along with any associated data. Deleted data will not be recoverable.

5.3 Notwithstanding anything to the contrary within any other Vysiion documentation, scheduled maintenance takes place on a monthly cadence. Advanced notification of maintenance activities is provided on the status page (available at https://status.FortiSASE™.com/) and Customer may subscribe to receive updates. In the event that, the integrity of the Service is at risk, Vysiion may perform emergency maintenance actions at its sole discretion and Vysiion will use reasonable efforts to inform affected Customers within one hour (1) ahead of the start of the maintenance activity.

5.4 The Customer acknowledges and agrees that: (a) the Service helps to prevent, find or eliminate malware and security breaches but it is technically impossible to guarantee 100% email or network security as no security device or service can guarantee full or unbreakable security or the blocking of all known malicious activity; and (b) Vysiion accepts no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect malware, malicious activity or for false positives including security breach, data loss, data corruption, and service interruptions and/or degradations of the Customer's network, systems.

5.5 The Customer acknowledges and agrees that:

5.5.1 the Service is designed to supplement and support, but not to replace, the implementation of an effective end-user computer usage policy by the Customer across its organisation.

5.5.2 logs are retained for seven (7) days. If the Customer requires their logs to be retained for longer than this period, the logs will be outsourced to a third-party., For the avoidance of doubt, retaining Customer logs for longer

than seven (7) is outside of the scope of this Service .

5.5.3 each FortiSASE™™ POP can support up to seven (7) seven dedicated IP addresses.

5.6 The Service provides an annual data transfer entitlement per Customer tenant of bytes received and sent (the "Data Transfer Entitlement"). The Customer's Data Transfer Entitlement is calculated from the combined value of each active Subscription.

Per Licence	Gigabytes Per Annum
FortiSASE™ User	250
FortiAP	500
FortiBranchSASE	500
FortiExtender	500
FortiSASE™ Branch OnRamp	50000

5.6.1 The entitlement period is three hundred and sixty-five (365) days running concurrent with the Customer's annual FortiSASE™ subscription ("Entitlement Period"). At the end of the Entitlement Period all calculations described herein are reset.

5.6.2 Comprehensive Tier- Excess Usage*:* If the Customer exceeds the Data Transfer Entitlement, for the Comprehensive Tier only, Vysiion reserves the right to limit the Customer's Data Transfer Usage for the remainder of their subscription. Customer will receive a limited daily allocation (the "Daily Enforcement Allocation") and Customer will be notified of the value of the Daily Enforcement Allocation. Once the Daily Enforcement Allocation is exceeded during any subsequent twenty-four (24) hour period, the Service will not accept new data packets until the next day. All notifications will be visible to Customer on login to the FortiSASE™ portal.

5.6.3 The Daily Enforcement Allocation is calculated as follows: every thirty (30) days during the Entitlement Period, on a rolling basis, the Customer's Data Transfer cumulative usage is tracked. The maximum sample value is recorded (the "30 Day Maximum Observed Cumulative Value"). The Daily Enforcement Allocation is a thirtieth of the 30 Day Maximum Observed Value. For example,

30 Day Maximum Value = 300 Gigabytes / 30 = Daily Enforcement Allocation = 10 Gigabytes

5.6.4 Additional Data Transfer is available for purchase, in increments of 250 (two hundred and fifty) gigabytes and activation of same, removes any Daily Enforcement Allocation then in effect.

5.7 Unless otherwise specified, the Service will be delivered in English language and remotely.

5.8 By purchasing the Service, the Customer agrees to be bound by (i) Fortinet's terms and conditions and (ii) Fortinet's activation policy (together, "Fortinet EULA") and Fortinet's then current privacy policy available at https://www.fortinet.com/corporate/about-us/privacy.html (or such other site as designated by Fortinet).