SCHEDULE M: SERVICE DEFINITION FOR DEDICATED FIREWALL SERVICE

1. Service Description for Dedicated Firewall Service

Vysiion will provide to the Customer and manage Dedicated Firewall appliance(s). The Dedicated Firewall is Vysiion Equipment; ownership will not pass to the Customer. The Dedicated Firewall Service comprises of the following mandatory components, to the extent set out on the Order Form:

- Provision of firewall appliance(s) (in the form of Hardware/ Software and/or Licensing);
- Vysiion Implementation (to the extent that Non UTM firewalls are in scope);
- Vysiion Management.

1.1 Firewall Appliance

The firewall appliance(s) can be:

(i) a deployed single or High Availability (HA) pair of configured dedicated firewall devices with Next Generation Unified Threat Management (NG UTM) capability licensing; or

(ii) a deployed single or High Availability (HA) pair of configured dedicated stateful firewall devices (Non UTM) with basic firewalling capability licencing.

The Dedicated Firewall appliance throughputs and features are subject to the model specification; the model will be as specified on the Order Form. The Customer is referred to the relevant vendor's website for specification details.

The following capabilities can be provided as part of the Dedicated Firewall Service, and is dependent on the vendor and licencing that is being taken out:

- Anti-Virus
- Application Control
- Intrusion Prevention
- Content Filtering
- Data Loss Prevention
- Threat Prevention
- User Identity
- Deep Packet Inspection*

**The inspection of encrypted (SSL/TLS) traffic is not included as standard and will require a consultative service to appropriately scope the requirements. A certificate is also required to enable this functionality, which can either come from the firewall vendor or provided by the customer from their own internal Certificate Authority. DPI can impact the performance of a firewall and so the hardware must be suitably specified for this to avoid potential performance issues.*

Further information around the devices and licencing can be provided on request.

The Customer recognises that a managed dedicated firewall is part of an overall security policy and does not guarantee total security.

1.1.1 Vendor Licensing

Licensing for the firewalls is provided as set out on the Order Form. The period of licensing set out on the Order Form is a fixed period calculated from the date of license activation set forth by the vendor (which can be confirmed upon request by the Customer to sales@vysiion.co.uk). Upon expiry of this period, licensing will need to be renewed to cover the remainder of the Initial Term or such longer period that the Customer may elect. The Customer shall be responsible for renewing vendor licensing and it is recommended that the Customer contacts their account manager not less than ninety (90) days prior to expiry of the licensing period to discuss renewal options. With respect to vendor licensing, Vysiion's obligation shall be limited to putting the relevant licensing in place.

1.2 Vysiion Implementation

Vysiion shall work remotely to complete the configuration of any non-UTM Dedicated Firewalls as follows, subject to maximum of two (2) Days' worth of resource. Day being a cumulative amount of time of not less than seven and a half hours spent working on the project during Normal Business Hours.
For implementation of NG UTM firewalls, the Customer will be required to contract with Vysiion for its Next Generation Managed Firewall Implementation Service (see Schedule D).
For the avoidance of doubt, the Customer shall be responsible for the physical installation of firewall devices unless the Customer has contracted with Vysiion for an installation service in respect of the firewalls such as Field Services as set out in Vysiion's Service Document for Professional Services.

1.2.1 Non UTM Firewall Implementation

The Dedicated Firewall(s) is pre-configured and is shipped to the Customer Site for self-installation unless the Customer has contracted with Vysiion for an installation service (such as Smart Onsite Install) in respect of the Dedicated Firewall appliance(s). A basic level of configuration and security policy development in consultation with the Customer is included. It will be the Customer's responsibility to provide the firewall policies during the configuration stage and notify Vysiion of any requested changes to such firewall policies during the Contract duration. Additional charges will apply where Vysiion is required to amend any configuration due to the Customer updating its firewall policies and will be scoped and quoted for by Vysiion at its then-current rates. Vysiion maintains full access to the firewall and carries out management using secure protocols (SSH HTTPS etc.) via the publicly visible interface. Vysiion will provide the Customer with the firewall configuration file, upon request. The Customer will not be provided with access to the firewalls. Four (4) security zones are included within the following three (3) categories: trusted, un-trusted and De-Militarized Zone. Any additional VLAN's required to extend security zones to Customer Site(s) are not included.

This service includes up to ten (10) Branch Office (Site to Site) IPSec VPNs. The number of SSL or IPSec dialup remote access connections will be limited by the firewall appliance provided; however, the number of VPN configuration sets (portals/domains) is limited to three (3) regardless of the method. It is the Customer's responsibility to ensure the client software/remote VPN device is configured correctly.

1.3 Vysiion Management

Vysiion management comprises of:

- 24x7x365 remote support from the Vysiion Service Desk
- Change Management

The Customer shall undertake reasonable on-site troubleshooting activities as requested by Vysiion.

A total of ten (10) hours of engineering time per calendar month to effect changes to the Firewall Appliances 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.*

The Service is managed by the Vysiion Network Operations Centre and monitored 24x7 for availability, CPU and memory. No security monitoring is included (such as alerts for policing traffic blocking or failed access attempts).

2. Service Demarcation Point (SDP)

The Dedicated Firewall SDP is the point up to which Vysiion's Dedicated Firewall service obligations apply and the Dedicated Firewall service level covers. The Customer-facing Ethernet Port(s) on the Firewall appliance will be the SDP.

3. Target Service Commencement Date

Dedicated Firewall Service (Non UTM)	25 Working Days [1,2]
Dedicated Firewall Service (NG UTM)	30 Working Days [1,2]

[1] From order acceptance if provisioned over an existing Smart Wires Service / from date of provision of any new Smart Wires Service required and may vary where Vysiion is not providing the internet service.

[2]The Target Service Commencement Date is subject to equipment vendor lead times and the Customer providing the required firewall policy input.

4. Service Level Agreement

Availability is defined as the firewall appliance(s) being able to process a network packet (not blocked by firewall policy), maintain a firewall session and remain connected to Vysiion's management platform. For HA pairs, if at least one firewall appliance is achieving these requirements then the Service shall be deemed Available.

	Target Availability
Dedicated Firewall Service – Single appliance	99.9%
Dedicated Firewall Service – HA Pair	99.99%

Service Credits

		Service Credit*
Measure	>0.1 below Target	10%

** The Service Credit is applied as a percentage of the Monthly Charge for the Dedicated Firewall Service*

5. Remote Access VPN

The Dedicated Firewall Service includes a Remote Access VPN capability, where users can establish a connection to the firewall appliance(s) over the internet to provide an on-demand connection to the Customer corporate network over an encrypted connection, relying on IPSec or SSL VPN technologies, as the vendor software allows.

Any Remote Access VPN connection should only be established using a secure method supporting multi-factor authentication (additional charges may apply), integrating an external identity provider via RADIUS, LDAP or SAML. Configuring the Remote Access VPN capability with local accounts, or other single-factor authentication solutions, is not permissible and shall not be done by the Customer.

It is the Customer's responsibility to ensure the client software and end user device is configured correctly, maintained, and updated. Where FortiClient is used to initiate a connection to the Remote Access VPN, Vysiion is unable to provide FortiClient software support without the Customer ordering the FortiClient Enterprise Management Server Service (see Schedule I).