SCHEDULE G: SERVICE DEFINITION FOR MANAGED DETECTION AND RESPONSE

1. Service Description for Managed Detection and Response

Vysiion's Managed Detection and Response (MDR) Service uses a proprietary software agent and platform to provide the Customer with Managed Detection and Response capability. The Service is delivered through the distribution of software agents on to endpoint devices (Laptops, Desktops and Servers) to minimise the risk of ransomware and malware compromise. The number of licences for the software agent will be set out on the Order Form. The CSOC team monitors events and activity on a 24/7 basis via a centralised platform. The software agent and platform interact to provide protection for the endpoint at the kernel level, reporting anomalies, malicious activity and endpoint telemetry to the platform. Customer access to the platform is provided to view the status of their endpoints. The platform is regularly updated; however, it provides continuous monitoring of the endpoints without the need for regular agent updates.

The Managed Detection and Response Service is only provided as a managed service, where:

- The Customer will be provided with multi-factor authentication-based access to the reporting portal for the number of users specified on the Order Form.
- Once the service has been set up, the Customer will be able to access the platform to observe the activity being produced by the endpoint protection product.
- Deployment responsibilities will depend on the type of implementation agreed on the Order Form. With self-implementation the Customer will be responsible for the deployment of the endpoint agents, and Vysiion will provide advice and assistance where necessary. With managed implementation Vysiion will be responsible for the deployment of the endpoint agents into the Customer's environment, and the Customer or their 3rd party service providers may be required to assist with the deployment of the software agents.
- The responsibilities of Vysiion and the Customer for the managed service are set out in the table below.

Responsibilities

The Parties' respective responsibilities are:

Vysiion Responsibilities	Customer Responsibilities
Discuss, document and feedback Vysiion's understanding of the configuration details, aligned to the Customer's business and technical requirements.	To engage in discussions with Vysiion as required to agree the policies and identify any specific exclusions for the service.
Deploy the central cloud management instance for the Customer.	
Configure policies and settings based on best practices and discussions/understanding with the Customer.	
Assist with the deployment of endpoint agents into the Customer's environment	Provide a list of the target endpoints and support relevant directory integration. Provide support, access, accounts and/or permissions for the role out of the agent to endpoints.
Test and confirm agents are reporting to the management platform.	Assist with troubleshooting any issues with agents not connecting/reporting.
Set up and manage configuration settings including any recommended rules/policies.	
Install and configure agent software on migrated and new endpoints.	Communicate new/updated/expired endpoints requiring agent installation.

Vysiion Responsibilities	Customer Responsibilities
Monitor and notify the Customer of any detected ransomware/virus.	Notify Vysiion of any reported virus/ransomware infections as soon as they are detected on any endpoint
Vysiion shall have no responsibility for any Malicious Code (including ransomware) infection.	
Provide advice and initial assistance to the Customer in relation to recovery following exploit of an endpoint	
Monitor and manage performance of the application and status (updates, downloads etc.).	Wherever reasonably possible approve requests from Vysiion to review, renew or advice on endpoint devices not reporting or functioning correctly.

2. Target Service Commencement Date*

Managed Detection and Response base configuration 5-10 Working Days, this excludes the role out of endpoint agents which is dependent on the number of endpoints, access to the endpoints and method of distribution available.

** from Order Acceptance.*

3. Service Level Agreement

This Service is not subject to a Service Level Agreement; however, Vysiion will use reasonable endeavours to alert the Customer of any detected events/issues within sixty (60) minutes of becoming aware of them.