SCHEDULE I: SERVICE DEFINITION FOR ENHANCED OPERATIONAL MANAGEMENT LEVEL – MICROSOFT CSP MANAGED

The Microsoft CSP Managed enhanced operational support level provides the relevant services detailed in this Schedule I for Microsoft Public Cloud environments. This enhanced operational support level provides a maintained environment consisting of Microsoft cloud components, based on the Functional Capability and Operation sections below, and configured by the Service Desk to the Customer's requirements.

Functional Capability

Vysiion will manage and support the following Microsoft Public Cloud environments where Vysiion is the Cloud Solutions Provider via which the applicable Microsoft Public Cloud environments are contracted by the Customer:

- Microsoft Azure (MA)
- Microsoft Dynamics 365 (D365)
- Microsoft 365 (M365)
- Microsoft Office 365 (O365)

The above shall be the Supported Items for the purpose of this Schedule.

Management of custom code is excluded from the Microsoft CSP Managed service, except where listed specifically under Operation.

Operation

The Microsoft CSP Managed enhanced operational support level components are as follows. Vysiion's responsibilities with respect to the Microsoft CSP Managed enhanced operational support level are described within the following table. The Customer is responsible for all management activities not included within Vysiion's responsibilities below. The Customer must raise all queries for Supported Items with Vysiion and not the Microsoft support desk directly.

Aspect	Vysiion's Responsibilities
Microsoft Azure Management These responsibilities are completed for Microsoft Azure environments only	**Global Azure Management** • Manage the Azure tenancy and its configuration settings on behalf of the Customer. • Annual analysis of an Azure environment to align the solution to current security, compliance, flexibility and scalability requirements. • Adding and removing Azure services that are managed by Vysiion upon request from the Customer. • Decommissioning of Azure services if requested by the Customer, based on Vysiion's ITIL compliant decommissioning process. • Configuration and management of the Azure tenancy environment, including any Azure options, features, or supported applications installed onto Azure. • Continuous (24x7x365) Azure Supported Public Cloud platform availability monitoring and determining whether Azure Supported Public Cloud operations are affected. • Continuous (24x7x365) Azure deployed resource service monitoring and alerting. • Delivery of approved Azure changes raised by Vysiion and the Customer.

Aspect	Vysiion's Responsibilities
	• Analysis and resolution of incidents raised for configured Azure alarms and warnings. • Manual analysis and resolution of incidents raised for configured Azure alarms and warnings that cannot be automatically resolved. **Access and Rights** • Manage Microsoft SSO authentication using the Azure AD tenant. • Manage Azure AD Connect to correctly provide the following features to the Customer: password hash synchronisation, pass-through authentication, federation using AD FS, synchronisation of AD objects with Azure, and robust health monitoring of on premise identity infrastructure. • Manage the management Users created in the Azure tenancy for Vysiion administrative, Customer administrative, data access, and Azure End User services purposes. • Manage the management Groups created in the Azure tenancy for Vysiion and the Customer. • Configure and manage Azure AD MFA policies for Azure administrators and users for access for supported hardware, operating systems, and applications. • Configure and manage Azure AD Conditional Access policies to Customer information on Microsoft 365 and Office 365. • Configure and manage Azure AD Self Service Password Reset. **Commercial** • Quarterly workload review and make recommendations on how service costs can be improved, and how services can be amended to provide greater functionality, availability, or performance. • Configure and manage Azure budgets and spending threshold notifications. **Health** • Monitor Azure Resource Health and notify the Customer of detected health problems. **Monitoring** • Azure infrastructure and cloud monitoring. • Raising incidents in the event of Azure infrastructure health and availability problems. • Remediating Azure infrastructure health and availability problems. • Installation and configuration of the required software needed to support Vysiion's service delivery of the managed services (including monitoring software and the setup of VM tools where applicable).
Microsoft 365 Management	**Global Microsoft 365 Management** • Work with the Customer to manage the Microsoft 365 tenancy and its operational configuration settings.

Aspect	Vysiion's Responsibilities
These responsibilities are completed for Microsoft 365 environments only	• Configure Delegated Administration on the Customer's Microsoft 365 account in order to provide Microsoft 365 Support. • Where escalation to Microsoft support is required, Vysiion will submit an incident and manage this incident with Microsoft. **Access and Rights** • Creation, maintenance and deletion of access to the Microsoft 365 components as required by the Customer. • Configure and manage Azure AD MFA policies for Azure administrators and users for access for supported hardware, operating systems, and applications. • Configure and manage Azure AD Conditional Access policies to Customer information on Office 365. • Managed Microsoft 365 SSO authentication using ADFS, Pass-through Authentication (PTA), or Password Hash Sync (PHS). **Anti-spam Management** • Configure the end user Microsoft 365 anti-spam solution based on Customer feedback and service improvement. • Configure ongoing end user access to Microsoft 365 anti-spam service. • Provide information in the End User Support Manual on end user configuration options available to users such as filtering, archiving, and secure messaging of confidential content. • Provide end user education on alerting Vysiion of detected spam suspicion. • Provide reporting on trends and metrics on successful anti- spam and unsuccessful anti-spam activities as part of the Monthly Service Management Reports. **Health** • Monitor Microsoft 365 Health and notify the Customer of detected health problems. **Manage Components** • Creation, maintenance and deletion of Microsoft 365 components, including the following: users, groups, mailboxes, calendars, message encryption policies, archive and legal hold policies, document and email access control policies, SharePoint sites, teams in Microsoft Teams, Yammer corporate network, information protection, and compliance policies (for Exchange, OneDrive, and SharePoint data). • Remediate Microsoft 365 application issues, directly or through notification to Microsoft 365 support teams. **Security** • Vysiion will be responsible for managing the mail security service under the Contract to cover: ○ SPAM filtering policies

Aspect	Vysiion's Responsibilities
	○ Malware filtering policies ○ Sending large email policies • Managing the Microsoft 365 Security & Compliance configuration. **User Management** • Creation, maintenance and deletion of authorised management user accounts on Microsoft 365. • Monitoring and remediation of credential replication with the corporate Active Directory environment using Azure AD Connect. • Creation and deletion of mailboxes (for users and groups). • Manage the configuration of Azure AD Self Service Password Reset. • Monitor Azure AD Self Service Password Reset. • Manage the Microsoft 365 user requirements on the Microsoft 365 environment. **Device Management** • Deployment of standard supported Workstation images created by Vysiion Professional Services using Windows 10 and Customer applications using Microsoft 365 services, or SCCM, or AutoPilot. • Carry out major application upgrades on Supported Items bi-annually: ○ For supported Microsoft software using Intune or AutoPilot and for Microsoft and third-party software using SCCM. • Perform Intune Workstation management for macOS and Windows Operating Systems including application approval, application deployment, device compliance policy, and security settings. • Perform Intune mobile device management for Android and iOS mobile devices including application approval, application deployment, device compliance policy, and security settings. **Enterprise Mobility and Security (EM+S)** • Securely linking Users' personal devices to Customer information and applications using Microsoft Intune. • Configure and manage Azure Rights Management encryption, identity, and authorisation policies to help secure Customer information. • Configure and manage Advanced Threat Analytics to detect suspicious activity and protect Customer systems from multiple types of advanced targeted cyber-attacks and insider threats. • Monitor EM+S Health and notify the Customer of detected health problems.
Microsoft Office 365 Management These responsibilities are completed for Microsoft Office 365 environments only	**Global Office 365 Management** • Work with the Customer to manage the Office 365 tenancy and its operational configuration settings. • Configure Delegated Administration on the Customer's Office 365 account in order to provide Office 365 Support. • Where escalation to Microsoft support is required, Vysiion will submit an incident and manage this incident with Microsoft.

Aspect	Vysiion's Responsibilities

	Access and Rights
	• Creation, maintenance and deletion of access to the Office 365 components as required by the Customer.
	• Configure and manage Azure AD MFA policies for Azure administrators and users for access for supported hardware, operating systems, and applications.
	• Configure and manage Azure AD Conditional Access policies to Customer information on Office 365.
	• Managed Office 365 SSO authentication using ADFS, Pass-through Authentication (PTA), or Password Hash Sync (PHS).
	
	Anti-spam Management
	• Configure the end user Office 365 anti-spam solution based on Customer feedback and service improvement.
	• Configure ongoing end user access to Office 365 anti-spam service.
	• Provide information in the End User Support Manual on end user configuration options available to users such as filtering, archiving, and secure messaging of confidential content.
	• Provide end user education on alerting Vysiion of detected spam suspicion.
	• Provide reporting on trends and metrics on successful anti- spam and unsuccessful anti-spam activities as part of the Monthly Service Management Reports.
	
	Health
	• Monitor Office 365 Health and notify the Customer of detected health problems.
	
	Manage Components
	• Creation, maintenance and deletion of Office 365 components, including the following: users, groups, mailboxes, calendars, message encryption policies, archive and legal hold policies, document and email access control policies, SharePoint sites, teams in Microsoft Teams, Yammer corporate network, information protection, and compliance policies (for Exchange, OneDrive, and SharePoint data).
	• Remediate Office 365 application issues, directly or through notification to Microsoft Office 365 support teams.
	
	Security
	• Vysiion will be responsible for managing the mail security service under the Contract to cover:
	  ○ SPAM filtering policies
	  ○ Malware filtering policies
	  ○ Sending large email policies
	• Managing the Office 365 Security & Compliance configuration.

Aspect	Vysiion's Responsibilities
	User Management • Creation, maintenance and deletion of authorised users either directly on Office 365 where credential replication is not implemented. • Monitoring and remediation of credential replication with the corporate Active Directory environment using Azure AD Connect. • Creation, maintenance and deletion of mailboxes (for users and groups). • Manage the configuration of Azure AD Self Service Password Reset. • Monitor Azure AD Self Service Password Reset. • Manage the Office 365 user requirements on the Office 365 environment.
Service Desk These responsibilities are completed for all Microsoft CSP Managed Services	• Where escalation to Microsoft cloud support is required, Vysiion will submit an incident to Microsoft cloud support and manage this incident with Microsoft.

Customer Pre-requisite Requirements

To start management of a Supported Item, Vysiion requires the following pre-requisites to be in place.

- Creation of Public Cloud Customer accounts.
- Creation of one Public Cloud administrative account for managed services On Boarding.
- Synchronisation of the Public Cloud with Vysiion's CSP licensing model.

To start management of the cloud environment, Vysiion requires the following pre-requisites to be fulfilled by the Customer during the On Boarding period.

- Conducting the On Boarding activities (as identified by Vysiion during the On Boarding process) including provision of information needed by Vysiion to correctly manage and support the Supported Items.
- Provision of design documentation for currently running Supported Items, where this exists.
- Provision of Configuration documents or CMDB information for currently running Supported Equipment that will be migrated to the Public Cloud and CMDB information for Supported Users, where it exists.

Customer Dependencies

For Vysiion to deliver the Microsoft CSP Managed enhanced operational support level, the following Customer dependencies exist. Failure of the Customer to meet these Customer Dependencies may affect the service Vysiion is able to deliver to the Customer, and Vysiion's obligations under the Microsoft CSP Managed service levels.

- Customer to provide documented naming conventions for all Supported Items.
- Customer to provide documented active Customer IT policies for all Supported Items at the time of starting the On Boarding process.
- Customer to provide Vysiion with advice in advance of any peculiar, special, or particular modifications made to the Supported Item. This includes advice on the Vysiion OS base level configuration as well as Vysiion's standard Microsoft CSP Managed practices.

- Customer will be responsible for documenting and maintaining any differing configuration and build requirements pertaining to the existing OS and application environment that is peculiar, special, or has had particular modifications applied.
- Customer to provide, in accordance with the timelines defined during the On Boarding activity, approval for patching events, the approved list of updates to be installed, and approved list of firmware to be installed on physical Supported Items.
- Customer must undertake application and pre-deployment compatibility testing before authorising Vysiion to migrate the Supported Items. Customer must re-undertake application and compatibility testing after migration has been conducted, prior to Vysiion taking on the Public Cloud components under management.
- Customer to have reviewed the compatibility of all custom and non-standard applications or line of business applications with the OS and service packs to be used.
- Customer to ensure that the Customer endpoints and management environments are secured, patched, and maintained in accordance with Good Industry Practice.
- Customer to ensure that the Customer applications layered on top of the OS are secured, patched, and maintained in accordance with Good Industry Practice for Supported Equipment that exists prior to the On Boarding activity.
- Customer must assess in advance the application suitability for virtualisation of their applications, and for use with the hypervisor used by the Microsoft Public Cloud.
- The Customer will work with Vysiion to replace all End of Life Supported Equipment before the arrival of the End of Life date.
- Customer to review the compatibility and suitability of the selected Supported Equipment configuration for its intended application usage.
- Vysiion shall retain administrative rights on the Supported Items in order to provide the Microsoft CSP Managed enhanced operational support level on Supported Items.
- Application installation or updates are performed by Vysiion for all Supported Equipment, as defined in the Operation section. Details of application installations or updates must be notified to the Customer prior to their application via the change management process.
- The Customer is responsible for all Supported Equipment to be protected by AV software. Supported Equipment not deployed with AV software are not covered by the Microsoft CSP Managed enhanced operational support level for virus infections free of charge.

The Customer is responsible for all Supported Equipment to be protected by backup software. Supported Equipment not deployed with backup software or SaaS based backups are not covered by the Microsoft CSP Managed operational support level for rebuild by Vysiion free of charge.

Service Education

Vysiion will provide education to Customer staff about the details of the service provided, and how to make use of the provided Microsoft CSP Managed service. Vysiion will provide the following service education for Supported Items.

Education	Timeline	Method
Raising incidents for faults/issues	On Boarding	Face-to-face CMDB document
Raising changes for system changes	On Boarding	Face-to-face CMDB document
Reporting	On Boarding	Face-to-face CMDB document
Requesting the creation of new Supported Items	On Boarding	Face-to-face

Education	Timeline	Method
		CMDB document
Requesting the addition of Supported Item resources	On Boarding	Face-to-face CMDB document
Disaster Recovery and Business Continuity design and process	On Boarding	Face-to-face CMDB document
Solution design documentation for Supported Items	First 3 months of BAU	CMDB document
Solution configuration documentation for Supported Items	First 3 months of BAU	CMDB document
Solution testing documentation for Supported Items	First 3 months of BAU	CMDB document

Accountabilities and Responsibilities

RACI

A responsibility assignment (RACI) matrix showing whether Vysiion, the Customer or any relevant third parties are Responsible, Accountable, Consulted or Informed in respect of a particular aspect will be drawn up to ensure a joint understanding. The RACI is bespoke to the Customer, is formalised during the On Boarding phase, and is documented in the CMDB.

The following table details who is responsible for high level ITIL-level RACI activities for the Microsoft CSP Managed enhanced operational support level. Some activities are shared between Vysiion and the Customer, where the Customer will be responsible for activities such as raising or approving change requests. Specific details are documented within the CMDB.

ITIL Process	Vysiion	Microsoft	Customer
Asset Management	RA	Not applicable	CI
Change Management	RA	C	RACI
Configuration Management	RA	C	CI
Event Management	RA	RAC	CI
Incident Management	RA	RAC	RCI
Patch Management	RA	RA	CI
Release Management	RA	RA	CI
Request Management	RA	RAC	RACI

The Customer is responsible for all RACI activities for areas that Vysiion is not responsible for. During the On Boarding activity the Customer shall identify key internal and 3rd line primary and back-up contacts to the Service Desk and promptly inform the Service Desk of any changes during the term of the Contract.

Service Requests

Service Requests are requested changes to a Supported Item or a request for an operational task made by the Customer. When the Customer submits a Service Request for a Supported Item, Vysiion will review the request and if it is required Vysiion will work with Microsoft to attempt to resolve the request.

All Service Requests will be reviewed, verified and are subject to approval by Vysiion, and Vysiion will confirm if additional charges apply. Additional charges will only apply to the extent that such Service Request do not fall within the scope of this Enhanced Operational Management Level as set out herein.

Service Requests will be carried out by Vysiion during Normal Business Hours. Should the Customer request that they be carried out outside of Normal Business Hours, additional charges in accordance with Vysiion's then-current Professional Services rates may apply.

Data Processing

When Vysiion provides the Enhanced Operational Management Level – Microsoft CSP Managed, this may result in Vysiion Processing Customer Personal Data. The following applies to the Processing of such Personal Data by Vysiion:

Subject Matter of Processing

The Personal Data (if any) that the Customer stores within the applications managed by Vysiion or the Customer's Active Directory.

Nature of the Processing

As reasonably required to provide the Microsoft CSP Managed Enhanced Operational Support Level in respect of the managed application.

Vysiion will not block, delete, correct, pseudonymise or encrypt any data. Vysiion has no responsibility for data accuracy in respect of the Customer data within the managed application.

Appropriate Technical and Organisational Measures

With respect to the requirement set out in the General Terms in Clause 10.15 at point (ii), the Customer agrees that as far as it is concerned the security measures set out in the Contract and Vysiion's maintenance of the ISO27001 (Information Security Management) standard (or any replacement or equivalent subsisting from time to time) (collectively the "Security Measures") fulfils the requirement of appropriate technical and organisational measures and the Customer agrees not to contend otherwise, recognising that the Charges for the Flex Manage directly relate to the Security Measures to be applied.