

Appendix 1

THIS STATEMENT OF WORK IS MADE ON [XXX]

BETWEEN

- (1) Sysgroup Trading Limited incorporated and registered in England and Wales with company number 4754200 whose registered office is at 55 Spring Gardens, Manchester. M2 2BY ("SysGroup" or "Supplier").
- (2) [Customer name], a registered company in England and Wales (XXXXX) of [Address] ("Customer")

together, the Parties.

BACKGROUND: The Parties have entered into a contractual relationship governed by the following documents, which collectively form the Agreement:

1. The Supplier's Standard Terms and Conditions: <https://www.sysgroup.com/wp-content/uploads/2025/06/Standard-TCsfinal.pdf>
2. The Services Terms, which outline the specific terms related to the delivery of Services <http://www.sysgroup.com/terms-and-conditions-services>;
3. The Acceptable Use Policy, which sets forth the terms governing the Customer's use of the Supplier's services and systems <https://www.sysgroup.com/acceptableusepolicy/>; and
4. The Operating Policy, which details the operational framework, including support processes, roles, and responsibilities <http://www.sysgroup.com/terms-and-conditions-support>.

The Agreement shall be the exclusive and binding terms governing the relationship between the Parties, and any amendments or updates shall be made in accordance with the terms set forth therein.

The Parties agree as follows:

1 INTERPRETATION

- 1.1.1 Unless otherwise stated in this SOW, all capitalised terms appearing herein shall have the meaning given to them in the other documents that form part of the Agreement as listed in the Background section.

2 DURATION

- 2.1 This SOW shall commence on the Services Commencement Date specified below and remain in place for the Subscription Term.

3 SERVICES AND DELIVERABLES

- 3.1 From the Services Commencement Date specified below:
 - 3.1.1 the Supplier shall provide the Services specified in this SOW to Customer in accordance with the terms of the Agreement.
 - 3.1.2 Unless otherwise stated in this SOW, Customer shall pay to the Supplier the Charges

specified in this SOW, in accordance with the terms of clause 9 of the Agreement.

3.1.3 Licences acquired on a usage or consumption basis will be charged on a used consumption basis in arrears based on the Third-Party Proprietor's Portal Pricing.

3.1.4 Professional Services shall be charged and paid in advance of the Services Commencement Date

3.2 Particulars of Services (where applicable) are described in section 4 below.

3.3 Services are described and quantified below

Support/Service		Unit Price	Quantity	Total Price
Project work	Day rate			
Total				

Service Commencement Date	[XXX]
Services Expiry Date	[XXX]
Subscription Term	The [] month period between Service Commencement Date and Services Expiry Date

By signing this Statement of Work, you confirm that you have the appropriate authority to enter into this Agreement on behalf of your organisation and agree to be bound by the terms and conditions of the Agreement

.....

Name Duly authorised signatory of

[]

Dated []



MICROSOFT 365	
Access to Microsoft 365	SysGroup will use GDAP controlled access permissions for the CUSTOMER (Microsoft 365 tenant) provided by the Microsoft portal. This will be used to support CUSTOMER with billing and service support.
Supported 365 Services	SysGroup will provide operational support services for the following standard non customized Microsoft 365 Services: • Tenant Administration ○ Domain management ○ DNS Management ○ Billing queries • EntraID ○ Sign-ins and Passwords. ○ User and Group management (not creation) • Exchange Online ○ Mail and Protection reports • OneDrive for Business • SharePoint Online (customer configuration not supported) • Teams (excluding Calling plans) • Device management ○ InTune ○ Defender for Business
Out of Scope	SysGroup will support CUSTOMER with all *First-Party Microsoft 365 services procured by CUSTOMER. All other works or services are excluded, and out of scope including but not limited to: • Deploying and provisioning of cloud resources. • Support for any customized configurations. • Creation or deletion of users and groups • Mail routing and 3rd party mail hygiene. • Deploying and provisioning of cloud networking services • Supporting on-premise synchronization. • Deployment and updates for InTune and Defender protected devices. • Purchase, deployment and harvesting of Microsoft 365 licenses • The usage and adoption of Office products • Training Services
Service Levels Microsoft 365	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy

MICROSOFT AZURE	
Access to Microsoft Azure	SysGroup will use Azure Lighthouse and CSP GDAP privileges as the controlled access method for support. In cases where Azure Lighthouse is not implemented, CUSTOMER will facilitate access for the SysGroup Operations Team to ensure efficient incident diagnosis and resolution. This will be achieved through one of the following methods: • Direct Access: Granting the SysGroup Operations Team the necessary permissions to access the CUSTOMER's web-based Microsoft Azure Portal or Azure PowerShell. • Screensharing: Providing real-time screenshare access to the Microsoft Azure environment. This access is critical to enable prompt troubleshooting and resolution of incidents, ensuring minimal disruption to the CUSTOMER's services.
Supported Azure Services	SysGroup will provide operational support services pursuant to its Support Operational Policy for the following Azure Services. · Support for First-Party Microsoft Azure Services (services configured via the Azure Portal) · Spend management for *First-Party Microsoft Azure services.
Out of Scope	SysGroup will support Customer with all *First-Party Microsoft Azure services procured by Customer. All other work or services are out of scope and excluded, including but not limited to: · Deploying and provisioning of cloud resources. · Deploying and provisioning of cloud networking services · Supporting Customer applications, operating systems or software running within virtual machines or supporting your specific configurations. · Supporting on-premise, non-cloud environments. · Patching operating systems, installed applications, software and application dependencies. · For the Spend Management making changes to the cloud environment or making custom API calls to obtain cloud usage information · Support Manual configuration policies. · Training Services
Service Levels Microsoft Azure	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.

*First Party as defined in the Microsoft Portal

PRIVATE CLOUD (SYSCLLOUD)	
Supported Private Cloud Services	SysGroup will provide a managed service for all infrastructure in its hyper-scale multi tenanted platform. This includes: • Compute: VMs, containers and server provisioning • Storage • Software Licencing • Networking • Edge security and threat management • Monitoring and alerting • Change Management
Out of Scope	SysGroup will support Virtual Machines (VMs) to the Operating System (OP) layer only. All other services are considered out of scope, and excluded from the Services including but not limited to: • Deployment of Applications on the VMs • Data on the VMs above the OS layer • Application management, development or support • Legacy system support • On-premise networking beyond the data canter • Endpoint security (unless specified in the SOW) • Third party application management or connectivity • Training Services
Service Levels Private Cloud	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.

CyberArk	
Access to CyberArk	SysGroup Operations Team is granted remote access to the customer CyberArk systems to provide remote administration and remediation. This is provided by the customer as part of the solution onboarding in a secure and auditable manner
Supported CyberArk Services	• 24x7 CyberArk Platform Continuous Monitoring: Ensuring the CyberArk platform is always operational and secure • System Management: This includes Safe, Component & Platform Management • CyberArk Account Onboarding & Management: Handling the setup and management of user accounts • Monthly Health Check Report: Providing regular updates on the system's health and performance • Technical Account Manager (TAM): A dedicated manager to oversee the service • Major and Minor Software Upgrades: Ensuring the system is always running the latest software • Disaster Recovery Testing: Regular testing to ensure the system can recover from any disaster Please note that User Management and Operating System Security patching (including Vault Servers) are not included in the scope of the service
Out of Scope	• User Management • Operating System security patching • Provision of Updated Licences and Media: For major version changes and interim minor releases • Professional Services: Any work deemed out of scope will be detailed in a statement of work and reviewed separately • Technical Advice and Consultancy: Requests for technical or product advice that do not relate to a service-affecting issue are not covered as part of the managed service • Any CyberArk services not expressly detailed in the supported CyberArk section
Service Levels CyberArk	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy

Zscaler	
Access to Zscaler	SysGroup Operations Team is granted remote access to the customer zScaler portal to provide remote administration and remediation. This is provided by the customer as part of the solution onboarding in a secure and auditable manner
Supported zScaler Services	• Ticket Portal Access • 24 x 7 x 365 Technical Support • Annual Health Check Report • Technical Account Manager (TAM) • Bypass & PAC file management • 24 x 7 x 365 Pro-Active Monitoring of Zscaler Service • Unlimited moves, adds, changes (8-6pm GMT) • Monthly Reporting via TAM • Management of all policies (Security, DLP, CASB, Cloud App etc.) • Client Connector Upgrade Management • Client Connector Application Policy and Forwarding Profile Management • Provisioning of new sites or capabilities • Compromised end point monitoring
Out of Scope	• Diagnostics of Technical Issues: Any diagnostics of technical issues that arise during implementation due to lack of maintenance, out-of-support software/hardware, or issues generated because of third-party migration • Setup of Devices: The setup of any devices is not included • Professional Services: Any tasks not mentioned as being in scope, including professional services, will be considered out of scope • Any zScaler services not expressly detailed in the in scope section
Service Levels zScaler	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy

CONNECTIVITY	
Access to Connectivity Infrastructure	SysGroup will be given full access to all connectivity infrastructure that they manage. Any changes to Hardware, Software or firmware will be completed using change control process. In the event physical access is required this will be arranged with prior agreement.
Supported Connectivity Services	SysGroup offers a comprehensive range of fully managed connectivity services. These services include: • Managed Internet Access ○ Purchasing, Provisioning, configuration ADSL, FTTC/P, Leased Line, MPLS, VPN and SDWAN • Managed WAN • Cloud Connections to SysGroup Private Cloud , Azure and AWS • Monitoring and alerting • Change Management • Managed Firewall ○ Firewall Installation and Configuration ○ Updates and Patching ○ Monitoring and threat analysis ○ Incident response support ○ Compliance reporting
Out of Scope	SysGroup will support the in-scope items above as stipulated by the agreed SOW. All other services are considered out of scope, and excluded from the Services including but not limited to: • Legacy / EOL system support • On-Premise Networking (unless stipulated in the SOW) • Endpoint security • End user connectivity • Legacy system support • Third party application management or connectivity • Training Services
Service Levels - Connectivity	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.

END USER SUPPORT	
Access for End user Support	SysGroup will be given full access to all Customer's infrastructure that they manage. Remote access will be used to support end users where required with SysGroup given the correct administrative privileges.
Supported End User Services	SysGroup shall deliver a comprehensive range of end user support services tailored to ensure end users have secure, seamless and reliable access to their work environments These services include: • Service Desk support and IT ticketing • Service request fulfilment • Account and Access management ○ User Onboarding and Offboarding ○ Password Resets ○ SSO and MFA • Incident management • Endpoint Device Troubleshooting • Operating System Support
Out of Scope	SysGroup will provide support the in-scope items above as specified in the SOW. All other services are considered out of scope and excluded. including but not limited to: • Legacy / End-of-Life (EOL) System Support. • On-Premise Networking: Unless stipulated in the Statement of Work (SOW) • Endpoint Security: Endpoint security services are not covered unless specified in the SOW. • Custom Software Development • Third-Party Application Support • Hardware Repairs. • Training Services:
SERVICE LEVELS –	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.

Backup (BaaS)	
	SysGroup will provide Backup as a Service (BaaS) to protect the following workloads: • Virtual Machines • Physical Servers • Applications (SQL, Oracle etc) • SaaS (M365, Azure, AWS etc) SysGroup BaaS offers the following benefits: • Automated Backups • Scalability • Ease of Use SysGroup BaaS follows the 3-2-1-1-0 Backup Rule: • 3 copies of data • 2 different types of media • 1 copy offsite • 1 copy offline or immutable • 0 errors after backup validation
Service levels - Backup	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.



Disaster Recovery (DRaaS)	SysGroup will provide Disaster Recovery as a Service (DRaaS) to protect the following workloads: • Virtual Machines • Physical Servers • Applicaitons (SQL, Oracle etc) • SysGroup DRaaS offers the following benefits: • Real-time or near real-time replication of critical data and systems to a secure environment • Failover: Instantly switch operations to a secondary site when a disaster occurs. • Failback: Restore operations to the primary infrastructure once the issue is resolved. • Periodic disaster recovery testing ensures readiness without disrupting live operations. • Automated workflows for disaster recovery processes, reducing manual intervention. • Tailored recovery plans based on the organization's specific Recovery Time Objective (RTO) and Recovery Point Objective (RPO) requirements.
Service Levels – Disaster Recovery	SysGroup will be working within the service levels defined in the SysGroup Support Operating Policy.

Professional Services	
Service Description	
Further details:	
In scope	
out of scope	